日 本 国 特 許 庁
PATENT OFFICE
JAPANESE GOVERNMENT

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: ２００１年 ３月１６日

出 願 番 号
Application Number: 特願２００１－０７６９１８

出 願 人
Applicant (s): ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００１年 ４月 ６日

特 許 庁 長 官
Commissioner,
Patent Office 及 川 耕 造

出証番号 出証特２００１－３０２７４５９

【書類名】　特許願
【整理番号】　0100227320
【提出日】　平成13年 3月16日
【あて先】　特許庁長官　及川　耕造　殿
【国際特許分類】　H04L　9/00
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　神谷　成樹
【発明者】
　【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内
　【氏名】　山下　雅美
【特許出願人】
　【識別番号】　000002185
　【氏名又は名称】　ソニー株式会社
【代理人】
　【識別番号】　100067736
　【弁理士】
　【氏名又は名称】　小池　晃
【選任した代理人】
　【識別番号】　100086335
　【弁理士】
　【氏名又は名称】　田村　榮一
【選任した代理人】
　【識別番号】　100096677
　【弁理士】
　【氏名又は名称】　伊賀　誠司

【先の出願に基づく優先権主張】

【出願番号】　特願2000-403472

【出願日】　平成12年12月28日

【手数料の表示】

【予納台帳番号】　019530

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9707387

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　配信方法及び配信システム

【特許請求の範囲】

【請求項１】　特定者に対し暗号処理の施されたディジタルデータを多地点配信する上流側システムと、配信を受けたディジタルデータに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルデータの配信方法であって、

上流側システムがその制御下において、

ディジタルデータを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の複数の鍵情報を生成する処理と、生成された複数の鍵情報をディジタルデータとは別の配信経路であって、鍵情報相互間においても別の配信経路となるものを用いて配信する処理と、暗号処理の施されたディジタルデータを配信する処理とを実行し、

当該ディジタルデータの配信を受ける下流側システムが、

正規の手続きによってのみ開封可能な復号サーバの制御下において、複数の配信経路を通じて配信を受けた複数の鍵情報を基に対応するディジタルデータの暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な出力装置の制御下において、上記復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する

ことを特徴とするディジタルデータの配信方法。

【請求項２】　特定者に対し暗号処理の施されたディジタルデータを多地点配信する上流側システムと、配信を受けたディジタルデータに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルデータの配信方法であって、

上流側システムがその制御下において、

ディジタルデータを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報をディジタルデータとは別の配信経路であって、相互においても別の配信経路となるものを用いて配信する処理と、暗号処理の施されたディジタルデータを配信する処理とを実行し、

当該ディジタルデータの配信を受ける下流側システムが、

正規の手続きによってのみ開封可能な復号サーバの制御下において、複数の配信経路を通じて配信を受けた一組の合わせ鍵又はその発生情報を基に対応するディジタルデータの暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な出力装置の制御下において、上記復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する

ことを特徴とするディジタルデータの配信方法。

【請求項３】　特定者に対し暗号処理の施されたディジタルデータを多地点配

信する上流側システムと、配信を受けたディジタルデータに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルデータの配信方法であって、

上流側システムがその制御下において、

ディジタルデータを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、当該複数の部分鍵又はその発生情報とこれら部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報をディジタルデータとは別の配信経路であって、相互においても別の配信経路となるものを用いて配信する処理と、暗号処理の施されたディジタルデータを配信する処理とを実行し、

当該ディジタルデータの配信を受ける下流側システムが、

正規の手続きによってのみ開封可能な復号サーバの制御下において、複数の配信経路を通じて配信を受けた複数の部分鍵又はその発生情報と、これらと組をなす合わせ鍵又はその発生情報を基に対応するディジタルデータの暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理の解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な出力装置の制御下において、上記復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する

ことを特徴とするディジタルデータの配信方法。

【請求項４】　特定者に対し暗号処理の施されたディジタルデータを多地点配信する上流側システムと、配信を受けたディジタルデータに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルデータの配信方法であって、

上流側システムがその制御下において、

ディジタルデータを対応する暗号鍵で暗号化する処理と、配信先である各特定者に固有の及び又はディジタルデータに固有の第２の暗号鍵を発生する処理と、上記第２の暗号鍵によって上記第１の生成された合わせ鍵又はその発生情報を暗号化する処理と、当該暗号化された第１の暗号鍵又はその発生情報と上記第２の暗号鍵又はその発生情報をディジタルデータとは別の配信経路であって、相互においても別の配信経路となるものを用いて配信する処理と、暗号処理の施されたディジタルデータを配信する処理とを実行し、

当該ディジタルデータの配信を受ける下流側システムが、

正規の手続きによってのみ開封可能な復号サーバの制御下において、複数の配信経路を通じて配信を受けた第２の暗号鍵又はその発生情報を基に、配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、第１の暗号鍵を復元する処理と、復元された第１の暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な出力装置の制御下において、上記復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する

ことを特徴とするディジタルデータの配信方法。

【請求項５】　特定者に対し暗号処理の施されたディジタルデータを多地点配信する上流側システムと、配信を受けたディジタルデータに施されている暗号処理を解除する下流側システムとの間で実行されるディジタルデータの配信方法であって、

上流側システムがその制御下において、

ディジタルデータを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の及び又はディジタルデータに固有の第２の暗号鍵を発生する処理と、上記第２の暗号鍵を基に一組の合わせ鍵を生成する処理と、第２の暗号鍵で暗号化された第１の暗号鍵又はその発生情報と上記第２の暗号鍵から生成された一組の合わせ鍵又はその発生情報をディジタルデータとは別の配信経路であって、相互においても別の配信経路となるものを用いて配信する処理と、暗号処理の施されたディジタルデータを配信する処理とを実行し、

当該ディジタルデータの配信を受ける下流側システムが、

正規の手続きによってのみ開封可能な復号サーバの制御下において、複数の配信経路を通じて配信を受けた一組の合わせ鍵又はその発生情報を基に第２の暗号鍵を復元して、配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、第１の暗号鍵を復元する処理と、復元された第１の暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理において生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な出力装置の制御下において、上記復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処

理でスクランブルが解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する

ことを特徴とするディジタルデータの配信方法。

【請求項６】　暗号処理の施されたディジタルデータの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを出力する出力装置とを備える電子配信システムにおける下流側システムであって、

上記復号サーバは、配信段階でディジタルデータに施された暗号処理を解除する暗号解除部と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成するスクランブル制御部と、上記暗号解除部で暗号処理が解除されたディジタルデータの唯一の出力先であって、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する復号化部と、復元されたディジタルデータの唯一の出力先であって、上記スクランブル制御部において生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力するスクランブル処理部とを備え、

上記出力装置は、上記受信サーバから入力されるディジタルデータに施されているスクランブル処理を、上記受信サーバから与えられたスクランブル解除鍵によって解除するスクランブル解除部と、上記スクランブル解除部でスクランブルが解除されたディジタルデータの唯一の出力先であって、当該ディジタルデータを所定の出力形態で出力する信号処理部と

を備えることを特徴とする電子配信システムにおける下流側システム。

【請求項７】　暗号処理の施されたディジタルデータの配信を受け所定の信号処理を実行する電子配信システムにおける復号サーバであって、

配信段階でディジタルデータに施された暗号処理を解除する暗号解除部と、

ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成するスクランブル制御部と、

上記暗号解除部で暗号処理が解除されたディジタルデータの唯一の出力先であって、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する復号化部と、

復元されたディジタルデータの唯一の出力先であって、上記スクランブル制御部において生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力するスクランブル処理部と

を備えることを特徴とする電子配信システムにおける復号サーバ。

【請求項８】　暗号処理の施されたディジタルデータの配信を受けて所定の信号処理を実行する電子配信システムにおける復号サーバの機能を実現する回路装置であって、

配信段階でディジタルデータに施された暗号処理を解除する暗号解除部と、

ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成するスクランブル制御部と、

上記暗号解除部で暗号処理が解除されたディジタルデータの唯一の出力先であって、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する復号化部と、

復元されたディジタルデータの唯一の出力先であって、上記スクランブル制御部において生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力するスクランブル処理部と

を備えることを特徴とする回路装置。

【請求項９】　コンピュータに、配信段階でディジタルコンテンツに施された暗号処理を解除する暗号解除処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成するスクランブル制御処理と、上記暗号解除処理で暗号処理が解除されたディジタルデータの唯一の出力先として、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する復号化処理と、復元されたディジタルデータの唯一の出力先として、上記スクランブル制御処理において生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力するスクランブル処理を実行させるプログラムを記録した

ことを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項１０】　暗号処理の施されたディジタルデータの配信を受け所定の信号処理を実行する電子配信システムにおける復号サーバであって、

配信段階でディジタルデータに施された暗号処理を解除する暗号解除部と、

上記暗号解除部で暗号処理が解除されたディジタルデータの唯一の出力先であって、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する復号化部と、

復元されたディジタルデータの唯一の出力先であって、スクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力するスクランブル処理部と

を備えることを特徴とする電子配信システムにおける復号サーバ。

【請求項１１】　暗号処理の施されたディジタルデータの配信を受けて所定の信号処理を実行する電子配信システムにおける復号サーバの機能を実現する回路装置であって、

配信段階でディジタルデータに施された暗号処理を解除する暗号解除部と、

上記暗号解除部で暗号処理が解除されたディジタルデータの唯一の出力先であって、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する復号化部と、

復元されたディジタルデータの唯一の出力先であって、所定のスクランブル鍵を用いディジタルデータの元データをスクランブル処理して出力するスクランブル処理部と

を備えることを特徴とする回路装置。

【請求項１２】　コンピュータに、配信段階でディジタルデータに施された暗号処理を解除する暗号解除処理と、上記暗号解除処理で暗号処理が解除されたディジタルデータの唯一の出力先として、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する復号化処理と、復元されたディジタルデータの唯一の出力先として、所定のスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力するスクランブル処理を実行させるプログラムを記録した

ことを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項１３】　配信を受けたディジタルデータに施されている暗号処理を解除する復号サーバであって、

ディジタルデータに付属する再生条件が満たされることを条件に、出力装置に出力されるディジタルデータの局所暗号化用のスクランブル鍵と当該スクランブル鍵で暗号化されたディジタルデータの出力装置側での局所復号化用の解除鍵を生成するスクランブル制御部

を備えることを特徴とする復号サーバ。

【請求項１４】　配信を受けたディジタルデータに施されている暗号処理を解除する復号サーバの機能を実現する回路装置であって、

ディジタルデータに付属する再生条件が満たされることを条件に、復号サーバから出力装置に出力されるディジタルデータの局所暗号化用のスクランブル鍵と当該スクランブル鍵で暗号化されたディジタルデータの出力装置側での局所復号化用の解除鍵を生成するスクランブル制御部

を備えることを特徴とする回路装置。

【請求項１５】　コンピュータに、配信を受けたディジタルデータに付属する再生条件が満たされることを条件に、復号サーバから出力装置に出力されるディジタルデータの局所暗号化用のスクランブル鍵と当該スクランブル鍵で暗号化されたディジタルデータの出力装置側での局所復号化用の解除鍵を生成するスクランブル制御処理を実行させるプログラムを記録した

ことを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項１６】　コンテンツを所定の出力形態で出力する電子配信システム対応の出力装置であって、

復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバ側から与えられたスクランブル解除鍵によって解除するスクランブル解除部と、

上記スクランブル解除部でスクランブルが解除されたディジタルデータの唯一の出力先であって、当該ディジタルデータを所定の出力形態で出力する信号処理部と

を備えることを特徴とする電子配信システム対応の出力装置。

【請求項１７】　コンテンツを所定の出力形態で出力する電子配信システム対応の出力装置に搭載可能な回路装置であって、

上記復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバ側から与えられたスクランブル解除鍵によって解除するスクランブル解除部

を備えることを特徴とする回路装置。

【請求項１８】　復号サーバから入力されるディジタルデータに施されているスクランブル処理を、所定のスクランブル解除鍵によって解除するスクランブル解除処理を、コンピュータに実行させるプログラムを記録した

ことを特徴とするコンピュータ読み取り可能な記録媒体。

【請求項１９】　特定者のみが再生できるように暗号処理の施されたディジタルデータの配信を受けて所定の信号処理を実行する復号サーバと、所定の出力形態でコンテンツを出力する出力装置とを備える電子配信システムにおける下流側システムの信号処理方法であって、

正規の手続きによってのみ開封可能な上記復号サーバが、配信段階でディジタルデータに施された暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、上記処理で暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力する処理とを実行し、

正規の手続きによってのみ開封可能な上記出力装置が、上記復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する

ことを特徴とする電子配信システムにおける下流側システムの信号処理方法。

【請求項２０】　暗号処理の施されたディジタルデータの配信を受けて所定の信号処理を実行する電子配信システムにおける復号サーバの信号処理方法であって、

正規の手続きによってのみ開封可能な上記復号サーバが、配信段階でディジタルデータに施された暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力する処理とを実行する

ことを特徴とする電子配信システムにおける復号サーバの信号処理方法。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明はディジタルデータの配信方法及び配信システムに関する。また、本発明は、ディジタルデータの配信方法及び配信システムの実現に必要な要素技術に関する。

【０００２】

【従来の技術】

ディジタル技術の進展に伴い、あらゆるディジタルデータ（文字データ（例えば、テキスト、記号、図形）、オーディオデータ（例えば、音声、楽曲）、ビデオデータ（例えば、静止画、動画）、オーディオデータとビデオデータの複合データ（例えば、映画、放送番組）、プログラムデータ、データベースデータその他のディジタルデータ）がネットワークや記録媒体を通じて配信されようとしている。

【０００３】

なお配信されるディジタルデータは、単一のデータファイルからなる場合もあれば、複数のデータファイルから構成される場合もある。またデータファイルに関しても、単一のコンテンツの情報のみを含むものもあれば、複数のコンテンツの情報が含まれるものもある。またコンテンツは複数のディジタルデータに分散される場合もある。

【０００４】

【発明が解決しようとする課題】

一方、ディジタルデータは完全な複製物を容易に作成できるため、不正行為（例えば、不正復号再生、不正複製、横流し）が行われると、非常に大きな損害が生じてしまう。このため、不正行為からコンテンツ提供者（例えば、コンテンツ制作者、配給権者、配信事業者）を保護する仕組み作りが急がれている。特に、制作に膨大な費用と人手を要し、資産価値の高いコンテンツ（例えば、映画）に関しては、不正行為によって莫大な損害が生じるため、不正行為が困難な仕組み作りが求められる。

【０００５】

しかし、防御能力が高いものは多大な設備投資を必要としたり、設備投資が比較的少なくて済むものは防御能力に問題がある等、コンテンツ提供者と受け手の双方が納得できるような仕組みは確立されていないのが現状である。

【０００６】

例えば、不正行為に対する耐性を高く保ち続けたり、より再現性の高い出力技術が現れた場合には適宜最新の技術を導入できることが望ましいが、現在提案されているビジネスモデルでは受け手側に必要な機能を全て出力装置内に設ける構成を採るため、技術寿命の短いものに合わせて出力装置自体の買い替えが必要となる。しかし、出力装置の短期間での買い替えを前提とするビジネスモデルでは、受け手側の理解を得ることができない。またその結果として、陳腐化した技術の置き換えが進み難く、ディジタルデータが不正行為にあう危険性が高まるという弊害がある。

【０００７】

このため、資産価値の高いコンテンツの提供がコンテンツ制作者に認められなかったり、ビジネスモデル自体が受け手側に受け入れられず、システムの運用を開始できない等の問題が生じている。

【０００８】

本願明細書は以上の課題を考慮し、ディジタルデータの配信段階から最終出力段階に至るまで不正行為が極めて難しく、しかも合理的な対価によって長期にわ

たって高い防御機能を維持できる配信方法及び当該方法を適用したシステム並びにそれらを実現する要素技術について提案する。

【０００９】

【課題を解決するための手段】

かかる課題を解決するため以下の手段を提案する。

【００１０】

（１）本願明細書で想定する配信モデル

以下の各手段では後述する処理を実行する上流側システムと下流側システムとで構成される配信モデルを想定する。

【００１１】

まず上流側システムとして、暗号処理の施されたディジタルデータを多地点配信するものを想定する。ここでの暗号化処理は、配信対象であるディジタルデータ毎に固有なもの（すなわち配信対象であるディジタルデータ毎に固有の暗号鍵で暗号化する）でも良いが、必ずしもこれに限らない。勿論、配信対象であるディジタルデータ毎に固有のものを使用すれば、不正行為が行われてもその被害が当該ディジタルデータ単位でしか生じないため、被害を最小化できる利点がある。ただし、システムの信頼性が高い場合や簡易な配信システムが望まれる場合には、複数のディジタルデータについて共通の暗号処理を採用する場合もあり得る。いずれの暗号化処理を採用するかは、ビジネス上の要請による。またここでの多地点配信には、放送による配信や通信による配信のように伝送媒体を通じて行う態様の配信の他、記録媒体を用いて物理的に行う配信も含まれる。

【００１２】

また、上流側システムは、ディジタルデータの暗号化に使用した暗号鍵の配信に際し、例えば以下に示すような方法のいずれかによって配信先やディジタルデータに固有の複数の鍵情報を作成し、それらをディジタルデータとは別の配信経路（媒体を物理的に異にするもの、又は、配信時間帯を異にするもの。以下同じ。）であって、鍵情報相互間においても別の配信経路となるものを通じて対応する配信先、すなわち下流側システムに配信する方式を採用する。すなわち、鍵情報を複数の経路を通じて配信することにより、いずれかの経路を通じて配信され

る鍵情報が盗まれた場合でも、他の全ての鍵情報が盗まれない限り被害の発生を防止できるようにする。なお配信される鍵情報は、暗号鍵そのものだけでなく、その発生情報（例えば、乱数）でもよい。また鍵情報は、暗号鍵を分割した合わせ鍵や部分鍵でもよい。因みに暗号化方式は共通鍵方式でも公開鍵方式でも良い。またこれらの複合方式でも良い。

【００１３】

上述の方法としては、例えば

１）暗号鍵を配信先毎に固有の分割パターンで分割し、一組（一対のみならず、３個以上の場合も含まれる。）の部分鍵を生成する方法

２）配信先毎に固有の異なる暗号鍵（請求項における第２の暗号鍵）を生成すると共に、当該暗号鍵でディジタルデータの暗号化に使用した暗号鍵（請求項における第１の暗号鍵）を暗号化したものを生成する方法

３）ディジタルデータ毎に固有の異なる暗号鍵（請求項における第２の暗号鍵）を生成すると共に、当該暗号鍵でディジタルデータの暗号化に使用した暗号鍵（請求項における第１の暗号鍵）を暗号化したものを生成する方法

がある。

【００１４】

なお配信先毎に固有の異なる暗号鍵（請求項における第２の暗号鍵）は、１つに限る必要はなく２つ以上使用しても良い。この場合、複数の第２の暗号鍵で第１の暗号鍵を２回以上（多重）暗号化すれば良い。いずれにしても、第１の暗号鍵が第２の暗号鍵で１回以上暗号化される点で違いはない。また第２の暗号鍵とは別の暗号鍵（例えば、配信先の違いによらず共通に使用する暗号鍵、ディジタルデータ毎に固有の暗号鍵、複数のディジタルデータに共通の暗号鍵、その他の暗号鍵）を組み合わせることで暗号処理を多重的に実行する等さまざまな暗号化手法が考えられる。

【００１５】

ここでの配信先毎に固有の分割パターンや配信先毎に固有の異なる暗号鍵は、配信者毎にほぼ普遍的に割り当てられている場合もあれば（ディジタルデータの違いによらず、比較的長期に同じ暗号鍵を使用する場合もあれば）、配信対象で

あるディジタルデータ毎にその都度割り当てられる場合もある。勿論、不正行為対策の観点からは後者が望ましい。

【００１６】

なお多地点配信の手法には、伝送網（ネットワーク）を用いて電子的に配信する方法の他、記録媒体を用いて物理的に配信する方法も含まれる。

【００１７】

次に、下流側システムとして、配信されたディジタルデータを復号する復号サーバと、復号されたコンテンツを所定の形態で出力する出力装置とが物理的に分離されているものを想定する。すなわち、復号サーバは、ディジタルデータとは別の複数の配信経路を通じて配信を受けた複数の鍵情報から元の暗号鍵を復元し、ディジタルデータに施されている暗号処理を解除する処理と、所定の信号処理の施されたディジタルデータを出力装置への出力用にスクランブル処理する処理とを実行するものを考える。

【００１８】

このように暗号処理の復号機能を出力装置とは別に設けるようにしたことにより、受け手側にとって設備の更新負担が少なくて済むシステム構成とできる。すなわち、配信システムの運用開始後に暗号方式の変更を行う場合にも、復号サーバだけを更新すればよく、暗号処理の復号とは関係のない出力装置については性能に支障のない限りそのまま使用できるようになる。同様に、出力装置をより性能の高いものに置き換える場合でも何らの問題のない復号サーバについてはそのまま使用できるようになる。かかる仕組みは長期的な運用コストを低減する上で効果的である。

【００１９】

もっとも、復号機能と出力装置を単に分離しただけでは不正行為に対して極めて無防備な配信モデルとなってしまうが、復号サーバと出力装置との間を流れるデータをスクランブル処理されたディジタルデータとすることにより、復号サーバと出力装置との間を流れるディジタルデータを不正に入手してもコンテンツ自体を入手できないようになっている。

【００２０】

なお、復号サーバや出力装置においても不正行為の起こり得ない仕組みを採用する。例えば、正規の手続き以外では復号サーバや出力サーバの筐体を開封できない仕組みや不正に開封すると動作しなくなる仕組みを採用する。また、復号サーバにおいて実行される特定の処理機能を集積回路化して処理の過程で現れる暗号鍵や生のディジタルデータが取り出されないようにする仕組みを採用する。ここで正規の手続きとしては、例えば開封する資格を有する者のみが保持する電子的な鍵や物理的な鍵を使用することが考えられる。また、不正に開封する行為としては、例えば筐体を破壊することが考えられる。

【００２１】

（２）配信モデルを実現する代表的な手段

以下、配信モデルを実現する代表的な手段について説明する。ここでの配信モデルは、前述のように上流側システムと下流側システムとで構成される配信システムを前提とする。また以下では、配信モデル全体からみた配信方法について説明する。なお上流側システムと下流側システムとは別の事業者によって構築される場合が一般的と予想されるが、ディジタルデータに施されている暗号処理を解除する処理までの処理までを上流側システムの事業者が受け持つような運用形態を排除するものではない。

【００２２】

上流側システムの運営形態には様々な形態が考えられる。例えば、単一の事業者が上流側システムを運営する形態や複数の事業者が共同して上流側システムを運営する場合が考えられる。このため、以下の各手段を構成する各処理は、単一の事業者によって行われる場合だけでなく、複数の事業者によって行われる場合もあり得る。

【００２３】

ここで単一の事業者としては、例えば、ディジタルデータの配給権を有すると共に、ディジタルデータの配信事業も行うものを想定する。なお単一の事業者には実質的に単一とみなすことができるものも含み得る。例えば、ある会社の税法上の子会社ではないが一定の資本関係の認められる関連会社や子会社が処理を分担して実施する場合も考えられる。もっともこれらは、後述するように、複数の

事業者による実施とも考えられる。

【００２４】

上流側システムが複数の事業者によって実施される場合、各処理機能がいずれの事業者に振り分けられるかはビジネス上の要請による。従って、各事業者で用いられる具体的なハードウェアの構成やソフトウェアの構成は各処理の組み合わせに応じて種々のものが考えられる。

【００２５】

例えば、ディジタルデータを暗号化するまでの処理と各配信先に応じた複数の鍵情報を生成する処理については配給権を有する事業者が実行し、配信事業者は暗号化されたディジタルデータの配信のみを行うようにすると、暗号鍵（マスター鍵）を知り得るのは配給権を有する事業者のみとできる。このため、かかる運営形態を採用する場合には、配給権を有する事業者にとって安全性を保持し易いシステムとできる。ここで配給権を有する事業者としては、例えばディジタルデータの制作者から配給権を得た事業者（コンテンツ制作者とは別の事業者である場合もあれば、コンテンツ制作者と同一の事業者である場合も含む。）が考えられる。

【００２６】

なお以下の各手段では、電子透かしについて言及していないが、不正行為の防止や流出経路の特定の観点からはディジタルデータを暗号化する前に、固有の電子透かしを入れておくことが望ましい。現実にはほとんどの場合に電子透かしが入れられると考えられる。

【００２７】

また、暗号化されたディジタルデータの配信に際し、配信事業者や伝送網の管理者が別途他の暗号処理を施すことは自由である。また、鍵情報を配信する場合にも実際は、電子証明書（信頼できる第３者機関である認証局がディジタル署名したもの）等によって相手先が真正な配信先であることを確認し、その上で相手方の公開鍵で鍵情報を暗号化しておくことが安全を期する上で望ましい。

【００２８】

なお以下の手段では、分割処理によって暗号鍵から直接得られる鍵を「合わせ

鍵」と、合わせ鍵を更に分割することで得られる鍵を「部分鍵」というものとする。もっとも、いずれの鍵も暗号鍵の一部分である点では同じである。また以下の手段では、暗号鍵を暗号化するのに使用する鍵を「多重鍵」というものとする。なお、暗号鍵の暗号化処理は１回のみならず２回、３回というように多数回重畳的に行う場合も当然含まれる。

【００２９】

また各手段において鍵情報を配信する場合には、鍵情報の伝送網にディジタルデータの伝送網と物理的に同じものを用いることも可能である。ただし、その場合にはディジタルデータと鍵情報とを同時刻に配信することはせず、それぞれの配信時間帯をずらし、実際上、別経路で配信するのと同様の状態で配信を行うことが望ましい。これは、ディジタルデータとその鍵情報とを同一の配信経路を通じて同時配信すると、１回の不正行為でディジタルデータと鍵情報の一部を同時に入手できるため、その分、ディジタルデータに施されている暗号が解除される危険性が高まるためである。

【００３０】

なお各手段のいずれの場合にも、下流側システムは配信を受ける鍵情報から暗号鍵を復元するのに必要な情報を予め知っているか、上流側システムから通知されるものとする。勿論、上流側システムから当該情報が通知されるタイミングは鍵情報の配信と同時でも良いし、別のタイミングでも良い。

【００３１】

（２－１）第１の手段

第１の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。なお、上流側システムは前述のように、ディジタルデータの配給権を有する事業者単独で運営される場合もあれば、当該配給権を有する事業者とディジタルデータの配信を実行する配信事業者とで運営される場合もある。また、下流側システムは前述のように、ディジタルデータに施されている暗号処理を解除する復号サーバと、ディジタルデータを所定の出力形態で出力する出力装置とで構成されるものである。これらは後述する他の手段においても同様である。

【００３２】

上流側システムがその制御下において、ディジタルデータを対応する暗号鍵で暗号化する処理と、上記暗号鍵を基に配信先である各特定者に固有の一組（一対のみならず、３個以上の組み合わせも含む。他の手段について同じ。）の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報をディジタルデータとは別の配信経路であって、相互においても別の配信経路となるものを用いて配信する処理と、暗号処理の施されたディジタルデータを配信する処理とを実行するものを提案する。

【００３３】

また下流側システム（個々の配信先毎に設けられる。）では、正規の手続きによってのみ開封可能な復号サーバの制御下において、複数の配信経路を通じて配信を受けた一組の合わせ鍵又はその発生情報を基に対応するディジタルデータの暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力する処理とを実行するものを提案する。

【００３４】

また正規の手続きによってのみ開封可能な出力装置の制御下において、上記復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行するものを提案する。

【００３５】

第１の手段は要するに、ディジタルデータの暗号化に使用した暗号鍵を、各配

信先（下流側システム）に固有の分割規則で分割して一組（例えば３個）の合わせ鍵を生成し、それらをディジタルデータとは別の配信経路であって、合わせ鍵相互においても別の配信経路となるものを用いて配信する方式と、配信を受けた鍵情報から復元された暗号鍵を用い暗号処理の解除されたディジタルデータにスクランブル処理を施したものを出力装置に出力する再生方式とを組み合わせたものである。

【００３６】

この第１の手段では信号処理の観点から説明しているが、これらの処理機能を備えるハードウェア構成によって実現することも可能であるし、同様の機能をソフトウェア処理として実現することも可能である。後述する他の手段についても同様である。この場合、ハードウェアやソフトウェア（コンピュータに該当処理を実行させるプログラムを記録した記録媒体、プログラム自体その他のプログラムプロダクト）は上流側システムと下流側システムのそれぞれについて用意する。なおハードウェアには、復号サーバや出力装置といった完成品の他、インターフェースボードや半導体集積回路等といった構成部品（請求項における回路装置）が考えられる。

【００３７】

かかる第１の手段を用いることにより、複数の配信経路を通じて配信される複数の鍵情報のうちいずれかが盗難されたとしても残る全ての鍵情報も盗難されない限り暗号鍵の流出を防止できる配信モデルを提供できる。特に、鍵情報をディジタルデータとは別の経路（上述のように同一の媒体を用いながら時間的に別の時間帯に配信する場合を含む。）で配信する場合には、鍵情報の一部を盗んだ不正行為者が暗号化されたディジタルデータをも入手した場合でも、暗号鍵の復元に必要な鍵情報はディジタルデータとは別に配信されるため、生のディジタルデータが復号化される事態をより困難にできる。

【００３８】

またこの第１の手段では、復号処理されたディジタルデータを局所的にスクランブル処理したものを出力装置に出力する方式を採用したことにより、復号サーバと出力装置を物理的に別の装置とする場合でも当該装置間において生のディジ

タルデータが流出するおそれを確実に回避できる配信モデルを提供できる。しかもその結果として、復号サーバや出力装置の開発負担を軽減できる。かくして、復号サーバや出力装置の価格の低下を実現でき、配信サービスの利用者にとっても導入し易いシステムとできる。また、長期の運用を考慮した場合にも最新の技術への置き換えが低い費用で進み易く、サービスの提供側にも利用者側にも好ましい仕組みを実現できる。かかる効果は他の手段についても同様である。

【００３９】

なお第１の手段では、ディジタルデータの暗号化に対応する暗号鍵が既に存在することを前提にするが、当該暗号鍵は上流側システム内で発生しても良いし、上流側システムの外部より与えられるものでも良い。ここでの暗号鍵は各ディジタルデータに固有のものでも良いし、複数のディジタルデータに共通のものでも良い。前者の鍵を使用する場合には、暗号鍵がたとえ最終的に解読されたとしてもその被害を当該ディジタルデータに限定することができる。もっとも、後者の鍵を使用する場合でも、比較的頻繁に鍵を変更することにより盗難時の被害が及ぶ範囲を限定できる。なお、このディジタルデータの暗号化に使用する暗号鍵についての説明は他の手段についても同様である。

【００４０】

因みに第１の手段における鍵情報の配信方法としては、例えば次のようなものを採り得る。例えば、一組の合わせ鍵の一部を伝送網（ネットワーク）を通じて配信し、その他を記録媒体を通じて配信する方法を採り得る。このように鍵情報の一部を有体物である記録媒体の形態で配信すると、鍵情報の盗難を発見し易く、不正行為に対する対抗策をいち早く実施できる。

【００４１】

また例えば、一組の合わせ鍵の一部を第１の伝送網（ネットワーク）を通じて配信し、その他を第２の伝送網（ネットワーク）を通じて配信する方法を採り得る。このように全ての鍵情報を伝送網を通じて配信すると、鍵情報の配信に要する時間的制約を少なくできる。また鍵情報の配信を経済的に実施できる。なお以上の伝送網（ネットワーク）を用いた鍵情報の配信に際しては、例えば電子証明書を使用して本人確認（配信先の確認）を行い、認証された配信先が公開する公

開鍵で暗号化した鍵情報を配信するなどの手法が望ましい。

【００４２】

また例えば、一組の合わせ鍵の一部を第１の記録媒体を介して配信し、その他を第２の記録媒体を介して配信する方法を採り得る。このように全ての鍵情報を有体物である記録媒体の形態で配信すると、鍵情報の盗難をより一層発見し易くでき、不正行為に対する対抗策をいち早く実施できる。勿論、２つの記録媒体には物理的に異なる媒体を使用する。言うまでもなく、記録媒体の種類や読み取り方式については同じでも、異なっても構わない。

【００４３】

ここで、合わせ鍵の配信に使用する記録媒体には、磁気読み取り方式の媒体（例えば、磁気テープ、フロッピーディスク、磁気カード）、光学読み取り方式の媒体（例えば、ＣＤ－ＲＯＭ、ＭＯ、ＣＤ－Ｒ、ＤＶＤ）、半導体メモリ（メモリカード（矩形型、正方形型など形状は問わない。）、ＩＣカード）その他が考えられる。当該記録媒体の配信には、郵便制度や宅配制度を使用する。現行の制度では、秘匿性の観点から書留郵便が選択される場合が多いと考えられる。この配信用の記録媒体についての記載は以下の各手段についても共通である。また、ディジタルデータの配信に用いる場合の記録媒体についても同様である。

【００４４】

また、前述の出力装置としては表示装置（例えば、モニタ装置、テレビジョン受像機、プロジェクタ装置、携帯型の電子機器）、印刷装置、スピーカ、記録媒体への記録装置等が考えられる。ここで、出力装置における所定の出力形態には、ディジタルデータが例えばビデオデータであれば、表示画面への表示、投影面への投影が考えられる。またディジタルデータが例えばオーディオデータであれば、スピーカを通じての出力が考えられる。勿論、オーディオデータとビデオデータの複合データであれば、その同時に２つの出力が行われる。

【００４５】

（２－２）第２の手段

第２の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【００４６】

上流側システムがその制御下において、ディジタルデータを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、当該複数の部分鍵又はその発生情報とこれら部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報をディジタルデータとは別の配信経路であって、相互においても別の配信経路となるものを用いて配信する処理と、暗号処理の施されたディジタルデータを配信する処理とを実行するものを提案する。

【００４７】

また下流側システム（個々の配信先毎に設けられる。）では、正規の手続きによってのみ開封可能な復号サーバの制御下において、複数の配信経路を通じて配信を受けた複数の部分鍵又はその発生情報と、これらと組をなす合わせ鍵又はその発生情報を基に対応するディジタルデータの暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理の解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力する処理とを実行するものを提案する。

【００４８】

また正規の手続きによってのみ開封可能な出力装置の制御下において、上記復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行するものを提案する。

【００４９】

第２の手段は要するに、ディジタルデータの暗号化に使用した暗号鍵を、各配信先（下流側システム）に固有の分割規則で分割して一組（例えば３個）の合わせ鍵とし、その一部（例えば２個）はそのまま配信し、その他（この場合１個）は例えば分割して複数の部分鍵を生成しこれを配信する方式と、配信を受けた鍵情報から復元された暗号鍵を用い暗号処理の解除されたディジタルデータにスクランブル処理を施したものを出力装置に出力する再生方式とを組み合わせたものである。勿論、これら鍵情報の配信には、ディジタルデータとは別の配信経路であり、かつ各鍵情報相互間においても別の配信経路となるものを使用する。

【００５０】

かかる第２の手段を用いれば、複数の配信経路を通じて配信される複数の鍵情報のうちいずれかが盗難されたとしても残る全ての鍵情報も盗難されない限り暗号鍵の流出を防止できる配信モデルを提供できる。しかもこの第２の手段の場合には、第１の手段よりも更に鍵情報の配信経路を増やせるため、より不正行為に対する安全性の高い配信モデルを提供できる。

【００５１】

なお合わせ鍵から一組の部分鍵を生成するのに用いる分割規則は、全ての配信先に共通の規則でも良いし、各配信先に固有の規則でも良いし、特定地域その他の条件で区分された配信先の集合毎に固有の規則でも良い。他の手段においても同様である。

【００５２】

なおここでの部分鍵の生成方法には、合わせ鍵の一部を更に分割する方法の他、合わせ鍵の一部を多重鍵する方法もある。後者の場合、暗号化された鍵情報とその暗号化に使用した暗号鍵が配信対象となる。同様の仕組みを採用する他の手段についても同様である。

【００５３】

因みに第２の手段における鍵情報の配信方法としては、例えば次のようなものを採り得る。例えば、合わせ鍵の一部を伝送網（ネットワーク）を通じて配信し、その他の合わせ鍵から生成される部分鍵の一部を伝送網（ネットワーク）で配

信し、残る部分鍵を記録媒体で配信する方法を採り得る。このように鍵情報の一部を有体物である記録媒体の形態で配信することで鍵情報の盗難を発見し易くでき、不正行為に対する対抗策をいち早く実施できる。なお言うまでもなく、記録媒体による配信はいずれの鍵情報でも良いし、任意の２種類の鍵情報をそれぞれ別の記録媒体で配信することもできる。

【００５４】

また例えば、一組の合わせ鍵の一部と、残る合わせ鍵から生成した部分鍵の全てを伝送網（ネットワーク）で配信する方法を採り得る。このように全ての鍵情報を伝送網（ネットワーク）を介して配信すると、鍵情報の配信に要する時間的制約を少なくできる。また鍵情報の配信を経済的に実施できる。なお以上の伝送網（ネットワーク）を用いた鍵情報の配信に際しては、例えば電子証明書を使用して本人確認（配信先の確認）を行い、認証された配信先が公開する公開鍵で暗号化した鍵情報を配信するなどの手法が望ましい。

【００５５】

また例えば、一組の合わせ鍵の一部と、残る合わせ鍵から生成した部分鍵の全てを記録媒体で配信する方法を採り得る。このように全ての鍵情報を有体物である記録媒体を介して配信すると、鍵情報の盗難をより一層発見し易くでき、不正行為に対する対抗策をいち早く実施できる。勿論、鍵情報の配信に使用する記録媒体はそれぞれ媒体の形態が異なっていても良いし、読み取り方式が異なっていても良い。

【００５６】

（２－３）第３の手段

第３の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【００５７】

上流側システムがその制御下において、ディジタルデータを対応する暗号鍵で暗号化する処理と、配信先である各特定者に固有の及び又はディジタルデータに固有の第２の暗号鍵を発生する処理と、上記第２の暗号鍵によって上記第１の生成された合わせ鍵又はその発生情報を暗号化する処理と、当該暗号化された第１

の暗号鍵又はその発生情報と上記第２の暗号鍵又はその発生情報をディジタルデータとは別の配信経路であって、相互においても別の配信経路となるものを用いて配信する処理と、暗号処理の施されたディジタルデータを配信する処理とを実行するものを提案する。

【００５８】

また下流側システム（個々の配信先毎に設けられる。）では、正規の手続きによってのみ開封可能な復号サーバの制御下において、複数の配信経路を通じて配信を受けた第２の暗号鍵又はその発生情報を基に、配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、第１の暗号鍵を復元する処理と、復元された第１の暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータの元データをスクランブル処理して出力する処理とを実行するものを提案する。

【００５９】

また正規の手続きによってのみ開封可能な出力装置の制御下において、上記復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行するものを提案する。

【００６０】

第３の手段は要するに、ディジタルデータの暗号化に使用した暗号鍵（第１の暗号鍵）を第２の暗号鍵で暗号化してなる暗号鍵と、その暗号化に使用した第２の暗号鍵を、ディジタルデータとは別の配信経路を用い、かつ、各暗号鍵相互においても別の配信経路となるものを用いて配信する方式と、配信を受けた鍵情報

から復元された暗号鍵を用い暗号処理の解除されたディジタルデータにスクランブル処理を施したものを出力装置に出力する再生方式とを組み合わせたものである。

【００６１】

かかる第３の手段を用いることにより、複数の配信経路を通じて配信される複数の鍵情報のうちいずれかが盗難されたとしても残る全ての鍵情報も盗難されない限り暗号鍵の流出を防止できる配信モデルを提供できる。特に、鍵情報をディジタルデータとは別の経路（上述のように同一の媒体を用いながら時間的に別の時間帯に配信する場合を含む。）で配信する場合には、鍵情報の一部を盗んだ不正行為者が暗号化されたディジタルデータをも入手した場合でも、暗号鍵の復元に必要な鍵情報はディジタルデータとは別に配信されるため、生のディジタルデータが復号化される事態をより困難にできる。

【００６２】

なお第２の暗号鍵として配信先である各配信者に固有のものを用いる場合には、特定の配信者から全ての鍵情報（第２の暗号鍵と暗号化された第１の暗号鍵）を盗難しない限り、ディジタルデータに施されている暗号を解除できない。すなわち、ある配信者に宛てて配信された固有の第２の暗号鍵と、ある配信者に宛てて配信された暗号化された第１の暗号鍵を盗難したとしても、第１の暗号鍵を取り出すことはできない。勿論、暗号化されたディジタルデータも盗難しなければディジタルデータ自体の盗難はできない。なお、全てのデータを不正行為が発覚する前に盗難することは事実上困難であり、不正行為に強いシステムとできる。

【００６３】

また第２の暗号鍵としてディジタルデータに固有のものを用いる場合には、第２の暗号鍵と当該第２の暗号鍵で暗号化された第１の暗号鍵が盗難された場合でも、その被害を特定のディジタルデータ（勿論、暗号化されたディジタルデータも盗難されることが前提となる。）に限定できる。言うまでもなく、この場合も全てのデータを不正行為の発覚前に盗難することは事実上困難であり、不正行為に強いシステムとできる。

【００６４】

なお言うまでもないが、第２の暗号鍵として配信先である各配信者について固有であり、かつディジタルデータについても固有のものを用いれば、より盗難の難しいシステムとできる。上述のいずれの暗号鍵を採用するかは、配信対象であるディジタルデータの経済的価値やディジタルデータの運用ポリシーによる。

【００６５】

因みに第１の暗号鍵の暗号化は第２の暗号鍵で少なくとも１回行えば良く、他の種類の暗号鍵で暗号化する処理と組み合わせても良い。従って、第２の暗号鍵で暗号化する前に既に第１の暗号鍵が暗号化されていても良い。このような場合でも第１の暗号鍵が第２の暗号鍵で暗号化されていることに技術上の違いはない。

【００６６】

なお第３の手段における鍵情報の配信方法としては、例えば次のようなものを採り得る。例えば、暗号化された第１の暗号鍵を伝送網（ネットワーク）を通じて配信し、第２の暗号鍵を記録媒体を通じて配信する方法を採り得る。このように鍵情報の一部を記録媒体の形態で配信すると、鍵情報の盗難を発見し易く、不正行為に対する対抗策をいち早く実施できる。なお上述の場合とは反対に、暗号化された第１の暗号鍵を記録媒体を通じて配信し、第２の暗号鍵を伝送網（ネットワーク）を通じて配信する方法を採ることもできる。

【００６７】

また例えば、暗号化された第１の暗号鍵を第１の伝送網（ネットワーク）を通じて配信し、第２の暗号鍵を第２の伝送網（ネットワーク）を通じて配信する方法を採り得る。このように全ての鍵情報を伝送網を通じて配信すると、鍵情報の配信に要する時間的制約を少なくできる。また鍵情報の配信を経済的に実施できる。なお以上の伝送網（ネットワーク）を用いた鍵情報の配信に際しては、例えば電子証明書を使用して本人確認（配信先の確認）を行い、認証された配信先が公開する公開鍵で暗号化した鍵情報を配信するなどの手法が望ましい。

【００６８】

また例えば、暗号化された第１の暗号鍵を第１の記録媒体を介して配信し、第２の暗号鍵を第２の記録媒体を介して配信する方法を採り得る。このように全て

の鍵情報を有体物である記録媒体の形態で配信すると、鍵情報の盗難をより一層発見し易くでき、不正行為に対する対抗策をいち早く実施できる。勿論、２つの記録媒体には物理的に異なる媒体を使用する。言うまでもなく、記録媒体の種類や読み取り方式については同じでも、異なっても構わない。

【００６９】

（２－４）第４の手段

第４の手段では、配信システムを構成する上流側システムと下流側システムのそれぞれが以下の処理を実行するものを提案する。

【００７０】

上流側システムがその制御下において、ディジタルデータを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の及び又はディジタルデータに固有の第２の暗号鍵を発生する処理と、上記第２の暗号鍵を基に一組の合わせ鍵を生成する処理と、第２の暗号鍵で暗号化された第１の暗号鍵又はその発生情報と上記第２の暗号鍵から生成された一組の合わせ鍵又はその発生情報をディジタルデータとは別の配信経路であって、相互においても別の配信経路となるものを用いて配信する処理と、暗号処理の施されたディジタルデータを配信する処理とを実行するものを提案する。

【００７１】

また下流側システム（個々の配信先毎に設けられる。）では、正規の手続きによってのみ開封可能な復号サーバの制御下において、複数の配信経路を通じて配信を受けた一組の合わせ鍵又はその発生情報を基に第２の暗号鍵を復元して、配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、第１の暗号鍵を復元する処理と、復元された第１の暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータの元データを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理において生成されたスクランブル鍵を用い、ディジタルデー

タの元データをスクランブル処理して出力する処理とを実行するものを提案する。

【００７２】

また正規の手続きによってのみ開封可能な出力装置の制御下において、上記復号サーバから入力されるディジタルデータに施されているスクランブル処理を、上記復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブルが解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行するものを提案する。

【００７３】

第４の手段は要するに、第２の暗号鍵を例えば分割して一組（例えば３個）の合わせ鍵とし、それらを暗号化された第１の暗号鍵と共に配信する方式と、配信を受けた鍵情報から復元された暗号鍵を用い暗号処理の解除されたディジタルデータにスクランブル処理を施したものを出力装置に出力する再生方式とを組み合わせたものである。勿論、これら鍵情報の配信経路には、ディジタルデータとは別の配信経路であり、かつ各鍵情報相互間においても別の配信経路となるものを使用する。

【００７４】

かかる第４の手段を用いれば、複数の配信経路を通じて配信される複数の鍵情報のうちいずれかが盗難されたとしても残る全ての鍵情報も盗難されない限り暗号鍵の流出を防止できる配信モデルを提供できる。しかもこの第４の手段の場合には、第３の手段よりも更に鍵情報の配信経路を増やせるため、より不正行為に対する安全性の高い配信モデルを提供できる。

【００７５】

なお第２の暗号鍵から一組の合わせ鍵を生成するのに用いる方法としては、上述のように所定の分割規則で第２の暗号鍵を分割する方法の他、第２の暗号鍵を更に別の暗号鍵で暗号化して得られる鍵情報とその暗号化に使用した暗号鍵をも含む。因みに、分割規則は全ての配信先に共通の規則でも良いし、各配信先に固有の規則でも良いし、特定地域その他の条件で区分された配信先の集合毎に固有

の規則でも良い。またディジタルデータに固有の規則であっても良い。勿論、これら配信先についての規則とディジタルデータについての規則とを組み合わせることにより、より一段と鍵情報の流出し難いシステムを構築できる。

【００７６】

なおこの第４の手段で用いる第２の暗号鍵も第３の手段と同様のものを使用する。例えば、第２の暗号鍵として配信先である各配信者に固有のものを用いる。この場合、特定の配信者から全ての鍵情報（第２の暗号鍵から生成された一組の合わせ鍵と、第２の暗号鍵で暗号化された第１の暗号鍵）を盗難しない限り、ディジタルデータに施されている暗号を解除できない。すなわち、第３の手段よりもある配信者に宛てて配信された固有の第２の暗号鍵が盗難される危険性を一段と低減できる。

【００７７】

また第２の暗号鍵としてディジタルデータに固有のものを用いる場合には、全ての鍵情報が盗難された場合でもその被害を特定のディジタルデータ（勿論、暗号化されたディジタルデータも盗難されることが前提となる。）に限定できるのに加え、第２の暗号鍵が盗難される可能性自体をより一段と低下できる。

【００７８】

なお言うまでもないが、第２の暗号鍵として配信先である各配信者について固有であり、かつディジタルデータについても固有のものを用いれば、より盗難の難しいシステムとできる。上述のいずれの暗号鍵を採用するかは、配信対象であるディジタルデータの経済的価値やディジタルデータの運用ポリシーによる。

【００７９】

因みに第１の暗号鍵の暗号化は第２の暗号鍵で少なくとも１回行えば良く、他の種類の暗号鍵で暗号化する処理と組み合わせても良い。従って、第２の暗号鍵で暗号化する前に既に第１の暗号鍵が暗号化されていても良い。このような場合でも第１の暗号鍵が第２の暗号鍵で暗号化されていることに技術上の違いはない。

【００８０】

なお第４の手段における鍵情報の配信方法としては、例えば次のようなものを

採り得る。例えば、暗号化された第１の暗号鍵を記録媒体で配信し、第２の暗号鍵から生成された一組の合わせ鍵の一部を伝送網（ネットワーク）で配信し、残る部分鍵を記録媒体で配信する方法を採り得る。このように鍵情報の一部を記録媒体の形態で配信することで鍵情報の盗難を発見し易くでき、不正行為に対する対抗策をいち早く実施できる。なお言うまでもなく、記録媒体による配信はいずれの鍵情報でも良いし、任意の１種類の鍵情報を記録媒体で配信し、その他の鍵情報は伝送網（ネットワーク）を介して配信することもできる。

【００８１】

また例えば、暗号化された第１の暗号鍵と、第２の暗号鍵から生成された一組の合わせ鍵の全てを伝送網（ネットワーク）を通じて配信する方法を採り得る。このように全ての鍵情報を伝送網（ネットワーク）を介して配信すると、鍵情報の配信に要する時間的制約を少なくできる。また鍵情報の配信を経済的に実施できる。なお以上の伝送網（ネットワーク）を用いた鍵情報の配信に際しては、例えば電子証明書を使用して本人確認（配信先の確認）を行い、認証された配信先が公開する公開鍵で暗号化した鍵情報を配信するなどの手法が望ましい。

【００８２】

また例えば、暗号化された第１の暗号鍵と、第２の暗号鍵から生成された一組の合わせ鍵の全てを記録媒体を通じて配信する方法を採り得る。このように全ての鍵情報を記録媒体を介して配信すると、鍵情報の盗難をより一層発見し易くでき、不正行為に対する対抗策をいち早く実施できる。勿論、鍵情報の配信に使用する記録媒体はそれぞれ媒体の形態が異なっていても良いし、読み取り方式が異なっていても良い。

【００８３】

【発明の実施の形態】

（１）ビジネスモデル

（１－１）一般例

図１に本願明細書が想定するビジネスモデルの基本的な構成例を示す。このビジネスモデルは、ディジタルデータの送り手である配信者と、ディジタルデータの受け手である特定者とで構成される。なお図１は、配信者が、ディジタルデー

タの配給権を有する配給権者１とディジタルデータの配信事業を行う配信事業者２の二者で構成される場合を表わしている。これは配給権者と配信事業者が同一人である場合も少なくないと考えられるが、それ以上に複数人によって配信者が構成される場合も少なくないと考えられるためである。

【００８４】

また、配給権者１はコンテンツ制作者からコンテンツ、すなわちディジタルデータの配給権を譲り受けた者である場合の他、コンテンツ制作者自身である場合、配給権者とコンテンツ制作者の共同事業体の場合もある。他方、特定者には個人や事業者（例えば劇場事業者）が該当する。

【００８５】

上述したように、ここでは上流側システム（データの流れから見て上流側のシステムの意味）が配給権者のシステムと配信事業者のシステムで構成され、下流側システム（データの流れから見て下流側のシステムの意味）が特定者のシステムで構成される場合について説明する。

【００８６】

配信対象に想定するディジタルデータは、文字データ（例えば、テキスト、記号、図形）、オーディオデータ（例えば、音声、楽曲）、ビデオデータ（例えば、静止画、動画）、オーディオデータとビデオデータの複合データ（例えば、映画、放送番組）、プログラムデータ、データベースデータ、その他のディジタルデータがある。勿論、これらの付属情報（例えばメタデータと呼ばれるＩＤ（媒体上の識別情報）、撮影日時、場所、人物、状態等に関する情報がある。）も含まれ得る。

【００８７】

一般に、ディジタルデータの配信には、伝送帯域が広く大容量のデータを配信するのに適した高速配信用ネットワーク３を想定する（図１）。この図１においては、コンテンツ制作会社１から電子配信事業者２にコンテンツとしてのディジタルデータを送り、高速配信用ネットワーク３を介して、特定者Ａ，Ｂ等にディジタルデータを配信するシステムを示している。ただし、ＣＤ－ＲＯＭやＤＶＤその他の記録媒体による形態での配信を排除するものではない。高速配信用ネッ

トワーク３には、放送衛星や光ファイバその他の広帯域伝送網を使用する。これらは少なくとも下り方向について大容量の伝送が可能なものを使用する。もっとも、上り方向への伝送も可能な双方向伝送網を用いても良い。

【００８８】

高速配信用ネットワーク３には、図２に示したようなデータ構造のデータ８が配信される。ここで、図２のデータ８には鍵の絵８Ａを表しているが、これはネットワーク提供者（配信事業者でない）が自身の提供する通信サービスの秘匿性を確保するために独自に暗号鍵を掛ける場合を表している。従って、この鍵は掛けられない場合もある。

【００８９】

もっとも、ディジタルデータの不正行為に対する安全性を最優先する配給権者や配信事業者は、ネットワーク上でも独自にデータに暗号処理を施すネットワーク事業者を選択するであろうし、その中でもより安全性の高い暗号処理を実行するネットワーク事業者を選択するものと考えられる。なお図２においては省略しているが、実際にはデータ８を配信する上で必要なヘッダが存在する。

【００９０】

図２の破線で囲まれた中身の部分が上記電子配信事業者２から配信されるデータに相当する。図２の場合、当該データには、データ又はファイルの格納情報を示すファイルアロケーションテーブル（ＦＡＴ：File Allocation Table）８Ｂと、ディジタルデータの使用条件（配信先、配信先毎の再生可能期間及び再生回数その他の条件）を含む業務データ８Ｃと、映像データ８Ｄと、音声データ８Ｅとが格納されている。

【００９１】

ここで各データに掛けられている鍵の絵は、これら各データが配給権者や配信事業者（そのいずれかの一方によって、又はその両者の協動によって）の施した暗号処理によって保護されていることを表わしている。ここで、各データに施されている暗号鍵は一般に同じ暗号鍵が使用される。ただし、データの種別ごと（例えば映像データごと）に異なる暗号鍵を採用しても良いし、データの種別に係わらず各データごと（例えば、コーデックを異にする映像データや音声データご

と）に異なる暗号鍵を掛けることも可能である。

【００９２】

図２に示すように、この配信モデルでは、あるコンテンツをマルチフォーマットで配信する方式を採用する。すなわち、配信対象である１つのコンテンツについて符号化復号化方式（コーデック）を異にする複数種類の映像データや音声データを用意して配信する方法を採用する。図２の場合、ある映像コンテンツについてコーデック方式を異にする３種類の映像データが配信される様子を表している。ここでのコーデック方式としては、例えば、ＭＰＥＧ（Moving Picture Experts Group）、ウェイブレット（Wavelet）その他が考えられる。

【００９３】

このように映像コンテンツを複数種類のコーディック方式で符号化し配信するのは、配信を受ける特定者側のシステム構成に自由度をもたせるためである。これにより、特定者はディジタル配信サービスの利用のためだけに専用のコーデックシステムを採用せずに済み、自身の使い慣れたシステムをそのまま利用することができる。このように、マルチフォーマットによる配信方式は、配信者の側から見ると特定者（データの配信先）が特定のシステムを保有するものに限られない利点があり、特定者の側から見るとディジタルデータの選択範囲が限られないため既存の設備を有効活用できる利点がある。

【００９４】

音声データ８Ｅについても同様である。図２の場合、２種類のコーデック方式で符号化されたデータが格納されている。ここでのコーデック方式には、例えば、ＭＰＥＧその他がある。

【００９５】

なお図１のビジネスモデルの場合、特定者Ａと表した個人宅が受信可能なデータは、映像コーデックVCD_1で符号化された映像データと音声コーデックACD_1で符号化された音声データであるため、それらが配信を受けたデータ８の中からＦＡＴの情報を基に選択的に抽出される又は再生される。一方、特定者Ｂと表した事業者が必要とするデータは、映像コーデックVCD_2で符号化された映像データと音声コーデックACD_2で符号化された音声データであるた

め、それらが配信を受けたデータ８の中からＦＡＴの情報を基に選択的に抽出される又は再生される。もっとも常にマルチフォーマットで配信しなければならないわけではないし、配信先毎に必要とされるフォーマットの組み合わせの情報を配信しても良い。

【００９６】

以上が高速配信用ネットワーク３を介して配信を受けるディジタルデータについての説明である。次に、当該ディジタルデータに施されている条件付きアクセス処理（Conditional Access）、すなわちディジタルデータに施されている暗号処理を解除するのに必要な暗号鍵の配信経路について説明する。図１では、暗号鍵の配信経路として、広域ネットワーク（伝送媒体）４と記録媒体５の２つを用いている。すなわち、図１は、共通鍵を復元するのに少なくとも２種類の鍵情報を必要とする場合において、その一部を広域ネットワーク４を介して電子的に配信し、残る一部を記録媒体５を通じて物理的に配信する方式を採用する配信方式の一例を表わしている。

【００９７】

なお、ここでの広域ネットワーク４は双方向通信が可能な伝送網を想定している。例えば、公衆網（例えば、インターネット網、ＡＴＭ網、パケット通信網）や専用線網が考えられる。また、記録媒体５は前述の課題を解決するための手段にて述べたように、磁気読み取り方式の媒体、光学読み取り方式の媒体、半導体メモリその他を想定する。その配信に郵便制度や宅配制度を利用することも前述の通りである。

【００９８】

なお以下の説明では、ディジタルデータに施す暗号鍵は全ての配信先について共通であり、各配信先に個別に配信される一組の鍵情報は各特定者に固有であると想定する。これは特定者毎に固有の鍵情報を採用することで、ある特定者に宛てて配信された全ての鍵情報を入手しない限り、ディジタルデータに掛けられている暗号鍵を復元できないようにするためである。このような仕組みを採用することで、このビジネスモデルは、全ての鍵情報を不正に入手するのがより困難なもの又は全ての鍵情報を不正に入手するのに時間を要するものとできる。

【００９９】

因みに前述の場合には、各ディジタルデータの暗号化に使用する暗号鍵を全配信者に共通なものとしたが、各ディジタルデータの暗号化に使用する暗号鍵を各配信先毎に固有のものとすることもできる。また前述の場合には、各配信先に個別に配信される一組の鍵情報が各配信先に固有のものとしているが、各ディジタルデータに固有のものとすることもできる。

【０１００】

因みに、ディジタルデータに掛けられる暗号鍵は、配信対象であるコンテンツに固有なものであることが望ましい。これは前述のように全ての鍵情報が不正に流出しディジタルデータの復号に成功したとしても被害を特定のコンテンツに限定できるためである。勿論、当該暗号鍵がコンテンツ毎に固有であることは必須ではなく、複数のコンテンツについて共通の暗号鍵を使用することも考えられる。要はシステム全体として不正行為に対する秘匿性が高まれば良いのであって、個々の暗号鍵が特定の規則に限定されるものではない。また秘匿性の高さは配信対象であるコンテンツによっても異なり、配信者側のポリシーによっても異なる。

【０１０１】

次に配信経路について説明する。基本的に鍵情報の配信には、図１に示すように、ネットワークと記録媒体というように媒体を異にするものを想定する。これは各配信経路の有する以下の特質に基づくものである。

【０１０２】

まず、ネットワークの場合、鍵情報の配信を即時に実行できるという利点を有する。ただし、鍵情報が盗難された場合に発見が難しいという欠点がある。これに対し、記録媒体の場合、鍵情報の配信は特定者が入手するまでに所定の時間を要するという欠点を有するが、鍵情報の盗難を物理的に確認することができるため盗難を発見し易いという利点がある。

【０１０３】

そこで、本願明細書で想定する多くのビジネスモデルでは、ネットワークを介しての配信と、記録媒体による物理的な配信との組み合わせを想定する。もっと

も以上は一般的な理由によるものであり、ネットワークを使った配信でも不正行為のおそれがない場合や困難な場合には、全ての鍵情報をネットワークを介して配信すればよい。また、鍵情報の配信からディジタルデータの配信までに期間的な余裕がある場合には、鍵情報の全てを記録媒体を使用して配信することもできる。

【０１０４】

因みに、ディジタルデータの暗号処理に使用する暗号技術については技術的な制約はなく、出願当時知られている各種の技術は勿論のこと将来現れるであろう各種の技術についても適用できる。暗号方式を問わないため技術的な寿命の影響を受け難いビジネスモデルとできる。また、常に運用当時最高の技術を選択できるため、その分、不正行為に強いビジネスモデルとできる。

【０１０５】

また図１において広域ネットワーク４と記録媒体５との２つの経路を通じて配信される鍵情報は、課題を解決するための手段において説明したように、配信先毎に固有の分割パターンで分割された一組の合わせ鍵（部分鍵）の組、又は、配信先毎に発生された固有の多重鍵で暗号化された暗号鍵と多重鍵の組を一般には想定する。

【０１０６】

（１－２）具体例

図３に、具体的なビジネスモデル例を示す。これは映画コンテンツを電子的に配信するビジネスモデルについてのものである。この種のビジネスモデルは従来からその実現に向け各種のビジネスモデル案が提供されているが、映画コンテンツの配給権を有する事業者と配信を受ける劇場側の双方を十分に満足させるものはなく実用に至ったものはない。そこで、本願明細書の配信モデルを適用することを考える。

【０１０７】

この図３に示すビジネスモデルの場合、図１のコンテンツ制作会社１は映画製作会社１ａに変わり、ディジタルデータの配信を受ける特定者６，７は劇場Ａ、Ｂに変わる。なお、図３の場合、映画コンテンツに特有な構成として、映画製作

会社１ａから提供されるフィルム画像を電子画像に変換する工程（テレシネ工程：Film to Video Conversion）９を表している。また図では区別していないが、劇場Ａ、Ｂは大規模な映画館や、小規模な映画館や、いわゆるシネコンと呼ばれる映画館等が想定される。

【０１０８】

（２）配信システム例

上述のビジネスモデルを実現する配信システムの機能ブロック構成例を示す。なお各システム例は、課題を解決するための手段で説明した第１～第４の手段のいずれかに対応する。勿論、実施形態例であるから部分的には特定の機能に限定した記載もあるが、前述の通りこれらに限られるものではない。

【０１０９】

（２－１）第１の配信システム例

図４に、上述のビジネスモデルを実現するための第１の配信システム例を示す。なお第１の配信システム例は前述の第１の手段に対応する。当該システムは上流側システムと下流側システムとで構成される。ここでの上流側システムは、コンテンツの配給権を有する事業者１のシステムと電子配信事業者２のシステムの複合システムとする。勿論前述のように単一事業者のシステムを排除するものではないし、３者以上の事業者による複合システムを排除するものではない。一方、下流側システムはディジタルデータの配信を受ける特定者毎に固有のシステムとする。

【０１１０】

（２－１－１）概念構成

まず当該第１の配信システム例の概念構成を説明する。この第１の配信システムには、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０１１１】

（１）第１のモデル

第１のモデルとして見た上流側システムは、各ディジタルデータに固有の暗号鍵を発生する処理と、ディジタルデータを対応する暗号鍵で暗号化する処理と、

上記暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部を伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵又はその発生情報のうち残りの部分を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。

【０１１２】

一方、下流側システムは、伝送網を通じて配信を受けた合わせ鍵又はその発生情報の一部と記録媒体の形態で配信を受けた残りの部分とを基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０１１３】

第１のモデルは要するに、ディジタルデータの暗号化に使用した暗号鍵を、各配信先（下流側システム）に固有の分割規則で分割して一組の合わせ鍵を生成し、その一部を伝送網を通じて配信し、残りを記録媒体の形態で配信する方式を採用するものである。

【０１１４】

（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、伝送網を通じて配信を受けた合わせ鍵又はその発生情報の一部と記録媒体の形態で配信を受けた残りの部分とを基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０１１５】

このとき下流側システムの出力装置は、復号サーバから入力されるディジタル

データに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを採用する。

【０１１６】

第２のモデルは要するに、配信を受けた鍵情報から復元された暗号鍵を用い暗号処理の解除されたディジタルデータにスクランブル処理を施して出力装置に出力する再生方式を採用するものといえる。

【０１１７】

なお、復号サーバで生成するスクランブル鍵とスクランブル解除鍵は、同じディジタルデータについては同じであっても良いし、暗号処理を解除する毎に固有の鍵を発生するようにしても良い。不正行為に対する対策としては後者の方が望ましい。

【０１１８】

また、出力装置としては表示装置（例えば、モニタ装置、テレビジョン受像機、プロジェクタ装置、携帯型の電子機器）、印刷装置、スピーカ、記録媒体への記録装置等が考えられる。

【０１１９】

ここで、出力装置における所定の出力形態には、ディジタルデータが例えばビデオデータであれば、表示画面への表示、投影面への投影が考えられる。またディジタルデータが例えばオーディオデータであれば、スピーカを通じての再生が考えられる。勿論、オーディオデータとビデオデータの複合データであれば、その同時に２つの出力が行われる。

【０１２０】

なお、以上の復号サーバや出力装置には、いわゆる完成品の他、該当機能を実現する回路装置（例えば、インタフェースボードや半導体集積回路等）のような構成部品も含まれる。

【０１２１】

（２－１－２）システム構成

図４の場合、上流側システムは、コンテンツサーバ１１と、コンテンツ符号化部１２と、暗号化部１３と、送出サーバ１４と、コンテンツ管理サーバ１５と、鍵発生部１６と、配信先管理サーバ１７と、合わせ鍵生成部１８と、書込部１９とから構成される。

【０１２２】

図４では、上流側システムにおけるこれらの各構成要素がいずれの事業者内システムに設けられるかをあえて明示していないが、これは各構成要素を各事業者にどのように配分するかはビジネス上の選択となるためである。なお各構成要素の配分又は配置の仕方は、他のシステム例についても共通する事項であるため、後段の「各システムで想定される運用形態」の項で別途説明する。

【０１２３】

一方、下流側システムは、受信サーバ３１と、読取部３２と、復号サーバ３３と、出力装置３４（デスクランブル部３４Ａ）とから構成される。このうち、復号サーバ３３は、更に復号機能部３５（復号化部３５Ａ、鍵復元部３５Ｂ、コンテンツ復号化部３５Ｃ、スクランブル部３５Ｄ）と、スクランブル制御部３６と、出力ログ管理部３７とで構成される。

【０１２４】

なお、これらの各構成要素はそれぞれ専用のハードウェアとして実現することも可能であるし、ソフトウェアの一機能として実現することも可能である。

【０１２５】

また図中、太線で示す矢印は伝送容量の大きい伝送路を表しており、細線で示す矢印は伝送容量の比較的小さい伝送路を表している。もっとも現時点で想定されるシステム構成であり、伝送容量が大きいか小さいかは相対的なものである。また現時点では細線の矢印で示す合わせ鍵の配信経路も伝送容量の大きいものとしても良い。

【０１２６】

（２－１－３）各機能部の構成

まず、上流側システムを構成する各機能部を説明する。コンテンツサーバ１１は、記録媒体（図４では磁気テープ）や伝送路を通じて提供を受けたディジタル

データの蓄積を主な機能とする装置である。このため大容量のストレージ装置を備える。なお当該サーバはコンピュータ構成を採る。

【０１２７】

すなわち、当該サーバは、制御機能と演算機能を実現する処理装置と、信号処理の実行に必要なデータを記憶する記憶装置と、外部からデータやプログラム及びコマンドを入力する入力装置と、処理結果を外部に出力する出力装置とを備える構成を採る。

【０１２８】

コンテンツ符号化部１２は、ディジタルデータの圧縮符号化その他の符号化処理を主な機能とする装置である。例えば、ＭＰＥＧ変換やＷａｖｅｌｅｔ変換その他の符号化処理が実行される。なお、符号化処理は一般に１種類だけが行われるのではなく、運用時に広く採用されている複数の符号化処理が行われる。この結果、１つのディジタルデータに対して複数の符号化処理データが生成される。なお音声や画像データに透かし情報を埋め込む処理は、例えばコンテンツサーバ１１とコンテンツ符号化部１２との間で実行される。このコンテンツ符号化部１２は、専用のハードウェアを用いて構成しても良いし、当該ハードウェアと同等の機能を実現させるプログラムがインストールされているコンピュータのソフトウェア上の処置として実現しても良い。

【０１２９】

暗号化部１３は、鍵発生部１６からコンテンツに固有の暗号鍵の提供を受け、当該暗号鍵を用いてコンテンツ符号化処理の終了したディジタルデータに暗号処理を施す装置である。ここで使用する暗号方式は運用時に広く採用されているものを用いれば良い。

【０１３０】

例えば、ＤＥＳ（Data Encryption Standard）、ＦＥＡＬ（Fast Data Encipherment Algorithm）その他の暗号処理が実行される。ここでの暗号処理は、業務データとコンテンツデータのそれぞれについて個別に実行される。参考までに言及すると、コンテンツデータについての暗号処理は、コンテンツ符号化部１２で生成された各符号化データ毎に実行される。

【０１３１】

なお暗号化部１３も、専用のハードウェアを用いて構成してもよいし、コンピュータに同等の機能を実現させるソフトウェアの処理機能として実現してもよい。

【０１３２】

送出サーバ１４は、特定者のみが視聴又は記録できるように暗号化処理の施された（条件付きアクセス処理が施された）ディジタルデータをストレージ装置に蓄積する機能と、配信スケジュールに従って高速配信用ネットワーク３に出力する機能とを実現する装置である。ここでの出力機能は、広帯域伝送機能やレートコントロール機能を備える送信装置で実現される。

【０１３３】

高速配信用ネットワーク３を用いたデータの配信は現在のところ夜間を利用した蓄積型の配信を想定しているが、伝送速度の向上が期待される将来においてはストリーミング配信等も想定する。

【０１３４】

なお、ディジタルデータの配信を記録媒体の形態で実行する場合、前述した出力機能はディジタルデータを所定の記録媒体に格納する記録装置で実現される。

【０１３５】

コンテンツ管理サーバ１５は、コンテンツサーバ１１と通信し、新たに受付けたコンテンツの登録処理やコンテンツの検索処理、ファイル分割処理その他を実行する装置である。当該サーバもコンピュータ構成を採る。当該サーバではコンテンツ毎に発生された暗号鍵情報が管理される。例えば、コンテンツと対応する暗号鍵との関係がデータベースとして管理される。

【０１３６】

鍵発生部１６は、配信対象であるディジタルデータ毎に固有の暗号鍵を生成する手段である。暗号鍵の発生に使用される暗号方式は運用時に広く採用されているものを使用する。すなわち、不正な解読が困難な最新の暗号化技術に従う。

【０１３７】

配信先管理サーバ１７は、コンテンツ毎に配信先と配信条件その他の業務デー

タや配信先毎に生成した暗号鍵の情報をデータベースにより管理する装置である。ここでの配信条件には使用可能期間、出力可能回数その他の情報が含まれる。また当該サーバもコンピュータ構成を採る。

【０１３８】

配信先管理サーバ１７は、コンテンツ配給権者１のシステムにのみ設ける場合、電子配信事業者２のシステムにのみ設ける場合、両者のシステム内に設ける場合その他が考えられる。これは各配信先に固有の鍵情報を誰が配信するかはビジネス上の選択事項だからである。ただし、鍵情報を知り得る事業者は少ないほどシステム全体からみた秘匿性は高まることは言うまでもない。一般にはコンテンツ配給権者１のシステム内に配置されるものと思われるが、ビジネスの運営形態に応じて電子配給事業者その他の事業者のシステム内に配置される場合もあり得る。

【０１３９】

図４その他の図面における配信先管理サーバ１７は、下流側システムの出力ログを上り回線（一般にはインターネットや電話回線その他の通信回線を使用する。）を通じて受信できるように構成されている。配信先管理サーバ１７は、当該出力ログに基づいて配信先（受信者側）の出力履歴（出力日時、出力回数、期間、付帯情報（トラブルの有無、コンテンツ視聴者の数や年齢層など）その他）を管理する。このため、配信先管理サーバ１７は、不図示のデータベースや出力履歴管理機能部を備える。

【０１４０】

もっとも、これらデータベースや出力履歴管理機能部は、配信先管理サーバ１７と別に設けられていても良い。なお出力ログの集計処理（統計処理も含む。）や分析処理は、出力ログの通知を受けた上流側システムにて実行しても良いし、下流側システムが予め実行した結果を送信するものとしても良い。

【０１４１】

このように下流側システムの出力ログ（実行事実）を上流側システムで管理することにより、コンテンツの流通状況を監視可能とできる。また、市場動向（興行成績、流行、傾向その他）を把握するのに使用できる。もっとも、ここでの上

流側システムは広義の上流側システムであり、ディジタルデータの配信権を有する事業者や電子配信事業者以外の事業者、例えばコンテンツの出力動向を調査する事業者であっても良い。

【０１４２】

なお、出力ログの受信は配信先管理サーバ１７が行わなくても良く、他の電子機器で受信しても良い。またここでの出力ログは、前述した全ての情報（例えば出力日時等）を表示する必要はなく、任意の１つ又は任意の組み合わせが通知されていても良い。ところで、図４を始め各図においては出力ログを下流側システムから上流側システムへ通知する場合を表わしているが、常に通知する必要はなく、また出力ログの通知を行わない配信システムを考えることも可能である。

【０１４３】

合わせ鍵生成部１８は、コンテンツ毎に生成された暗号鍵Ａを配信先毎に固有の分割パターンで分割し、一組の合わせ鍵Ａ１及びＡ２を生成する装置である。例えば、配信先となる特定者が１０００人いれば、１０００組の合わせ鍵Ａ１及びＡ２が生成される。生成された合わせ鍵は、合わせ鍵生成部１８によって配信先管理サーバ１７と所定の配信処理部に与えられる。このシステムの場合、合わせ鍵生成部１８は、合わせ鍵Ａ１をネットワークを介した配信用に不図示の通信部に与え、残る合わせ鍵Ａ２を記録媒体を介した配信用に書込部１９に与える。

【０１４４】

書込部１９は、通知を受けた合わせ鍵Ａ２を所定の記録媒体に書き込むための装置である。書込部１９には、記録媒体に応じた駆動機構が設けられる。記録媒体には、磁気読み取り方式の媒体、光学読み取り方式の媒体、半導体メモリその他の媒体が用いられる。なお、記録媒体の配信に必要な宛先情報は配信先管理サーバ１７から与えられる。前述の不図示の通信部についても同様である。ただし、通信部の場合にはネットワーク上のアドレスが与えられる。

【０１４５】

次に、下流側システムを構成する各機能部を説明する。受信サーバ３１は、特定者のみが視聴又は記録できるように暗号化処理の施された（条件付きアクセス処理が施された）ディジタルデータの受信機能と、配信を受けたディジタルデー

タをストレージ装置に蓄積する機能と、再生スケジュールに従って復号サーバ３３に出力する機能とを実現する装置である。ここでの受信機能は、受信データに含まれる誤り訂正等を行う機能も備える。

【０１４６】

なお、ディジタルデータの配信を記録媒体の形態で受ける場合、前述した受信機能はディジタルデータを所定の記録媒体から読み取る読取装置で実現される。

【０１４７】

読取部３２は、記録媒体の形態で配信される合わせ鍵Ａ２を記録媒体から読み取るための装置である。ここで駆動機構には、記録媒体に応じたものが用いられる。また、図中では表していないが、広域ネットワークを介して配信を受ける合わせ鍵Ａ１の受信用に通信部が設けられている。

【０１４８】

復号サーバ３３は、ディジタルデータに施されている暗号処理を解除する処理と、暗号が解除されたディジタルデータに施されている符号化処理を復号化する処理とを実行する一方で、復元された生のディジタルデータがそのまま装置外部に出力されないように局所的なスクランブル処理を施す装置である。

【０１４９】

復号サーバ３３は、専用のハードウェアを用いて構成しても良いし、コンピュータに同等の機能を実現させるソフトウェアの処理機能として実現しても良い。因みに当該復号サーバ３３は、悪意の特定者による不正行為からディジタルデータを保護するため、正規の手続き以外ではその筐体を開封できない仕組みや不正に開封すると動作しなくなる仕組みを採用する。これらの仕組みについては既存の技術を使用する。

【０１５０】

特に、復号機能部３５（復号化部３５Ａ、鍵復元部３５Ｂ、コンテンツ復号化部３５Ｃ、スクランブル部３５Ｄ）については、各機能ブロック間において重要な情報（暗号鍵や生のディジタルデータ）が流れるため、不正行為を排除するための対策が重要であり、当該機能ブロック部分を半導体集積回路化したり、正規な手続き以外ではその筐体を開封できない仕組みや不正に開封すると動作しなく

なる仕組みを採用する。

【０１５１】

ここで、復号化部３５Ａは、鍵復元部３５Ｂから与えられる暗号鍵を用い、受信サーバ３１から読み出されたディジタルデータに施されている暗号処理（条件付きアクセス処理）を解除する機能部である。当該機能は専用のハードウェアで実現することもできるし、ソフトウェア上の機能として実現することもできる。

【０１５２】

鍵復元部３５Ｂは、ネットワークを介して配信を受けた合わせ鍵Ａ１と記録媒体の形態で配信を受けた合わせ鍵Ａ２に基づいて、ディジタルデータに施されている暗号処理を解除できる暗号鍵を復元する機能を実現する機能部である。復元された暗号鍵は鍵復元部３５Ｂの管理下において所定の期間保持される。当該確認には不揮発性メモリ、ハードディスクその他の記録媒体が用いられる。

【０１５３】

また鍵復元部３５Ｂは、受信サーバ３１から読み出されたディジタルデータの暗号を復号するのに先だって、当該ディジタルデータに付属されている業務データ８Ｃを読み出し、当該業務データ８Ｃで定められている再生条件（使用条件）が各時点において満たされているか否かの判定も行う。

【０１５４】

ここで、鍵復元部３５Ｂは、再生条件が満たされるとき、復号化部３５Ａに暗号解除許可信号を与える一方、スクランブル制御部３６にスクランブル鍵の発生信号又は出力許可信号を与える。これに対し、鍵復元部３５Ｂは、再生条件が満たされないとき、復号化部３５Ａに暗号解除禁止信号を与えると共に、スクランブル制御部３６にスクランブル鍵の発生禁止信号又は出力禁止信号を与える。

【０１５５】

コンテンツ復号化部３５Ｃは、特定者毎が採用しているコーデック方式に対応するものが用いられる。当該機能も専用のハードウェアとして実現することも可能であるし、ソフトウェアの一機能として実現することも可能である。コンテンツ復号化部３５Ｃの信号処理の結果、暗号化処理前の生のディジタルデータが復元される。

【０１５６】

スクランブル部３５Ｄは、コンテンツ復号化部３５Ｃによって復元されたディジタルデータがそのままの形態で出力されることがないように、スクランブル処理を施すための装置である。当該機能も専用のハードウェアとして実現することも可能であるし、ソフトウェアの一機能として実現することも可能である。

【０１５７】

なお図４の場合、スクランブル制御部３６を復号機能部３５の外部においているが、スクランブル制御部３６を復号機能部３５内の一機能として設けることも可能である。

【０１５８】

スクランブル制御部３６は、鍵復元部３５Ｂによりスクランブル鍵の発生が許可された場合、スクランブル鍵とこれと対をなすデスクランブル鍵を発生する。なお鍵復元部３５Ｂからスクランブル制御部３６に与えられる許可信号は、単なる許可と非許可の情報だけでなく、出力日時や期間等の情報を含むものでも良い。またスクランブル制御部３６を図中破線で示すように、コンテンツ復号化部３５Ｃその他に対して外部接続する場合には当該機能部間で互いを認証し、相手側が真正であると認めた場合にのみスクランブル鍵が発行されるようにしても良い。

【０１５９】

なお、スクランブル鍵とデスクランブル鍵の発生方法には、コンテンツの違いによらずいつも同じスクランブル鍵等を発生する方法（固定的に記憶されているスクランブル鍵とデスクランブル鍵を出力する方法）と、コンテンツ毎に異なるスクランブル鍵等を発生する方法（新たなコンテンツの出力のたび生成され、所定の再生条件が満たされる間保持される方法）と、再生出力のたびに異なるスクランブル鍵等を生成する方法（コンテンツの暗号を解除するたびに異なるスクランブル鍵を生成する方法）とがある。不正行為に対する防御機能の観点からは、記載順に３番目の方法、２番目の方法、１番目の方法の順番で不正が困難になる。

【０１６０】

因みに、スクランブル制御部３６は、１つのコンテンツを出力する間にスクランブル鍵を定期又は不定期に切替える仕様を採用する場合にはディジタルデータの出力装置３４への出力中も適宜スクランブル鍵とデスクランブル鍵を発生する。

【０１６１】

また図４その他の図面では、スクランブル制御部３６から出力ログ管理部３７にスクランブル鍵等の発生状況を通知するように描かれていないが、かかる管理情報を出力ログ管理部３６に与えるようにしても良い。このような情報を出力ログ管理部３７に与えることで、スクランブル鍵等が不正に発生されたものか否かを監視できる。

【０１６２】

出力ログ管理部３７は、出力装置３４からの不正出力を監視するため、出力装置３４における出力ログを管理する装置である。当該機能も専用のハードウェアとして実現することも可能であるし、ソフトウェアの一機能として実現することも可能である。出力ログ管理部３７は、出力ログを通信回線を通じて上流側システムを構成する配信先管理サーバ１７に通知する。この結果、上流側システムでも別途、各特定者の再生出力状況を監視できる。また不正行為の発見にも利用できる。

【０１６３】

なおここでの出力ログは、下流側システムで発生した又は入力された生のデータを想定しているが、当該出力ログ管理部３７その他の装置において集計処理（統計処理）や分析処理されたものでも良い。因みに、出力ログの情報としてコンテンツ視聴者の数や年齢層などの付帯情報を含める場合には、当該情報が不図示の入力手段や処理装置から与えられるものとする。

【０１６４】

最後に、出力装置３４の構成を説明する。出力装置３４は、ディジタルデータに応じたものが用いられる。画像系であれば表示装置や投影装置が考えられるし、音声系であればスピーカーが考えられる。いずれにしても、出力装置３４は、その本来の機能部の他にデスクランブル部３４Ａを備える。

【０１６５】

デスクランブル部３４Ａは、復号サーバ３３から与えられるディジタルデータに施されているスクランブル処理を解除するための機能装置である。当該機能も専用のハードウェアとして実現することも可能であるし、ソフトウェアの一機能として実現することも可能である。当該デスクランブル部３４Ａは、半導体集積回路やボード部材で構成される。

【０１６６】

この出力装置３４の場合も、デスクランブル部３４Ａから出力される信号については、電子透かしのような静的な保護機能しか施されていないため、正規の手続き以外では出力装置の筐体を開封できない仕組みや不正に開封すると動作しなくなる仕組みを採用する。

【０１６７】

（２－１－４）ディジタルデータの配信動作

第１の配信システム例におけるディジタルデータの配信動作を簡単に説明する。当該システムでは、新たなディジタルデータがコンテンツサーバ１１に登録されると、コンテンツ管理サーバ１５の管理下において当該コンテンツに固有の暗号鍵が発生される。次に、作成された暗号鍵が合わせ鍵生成部１８に与えられ、各配信者に固有の分割パターンによって固有の合わせ鍵が生成される。

【０１６８】

ここで、各配信者に固有の分割パターンはコンテンツの違いにかかわらず同じものでも良いし、コンテンツ毎に異なる分割パターンを採用しても良い。いずれにしても、図４のシステム例では、特定者毎にコンテンツに固有の合わせ鍵が生成される。

【０１６９】

その後、生成された合わせ鍵Ａ１とＡ２がディジタルデータの送信に先立って事前に配信される。このシステムの場合、合わせ鍵Ａ１はネットワークを通じて、合わせ鍵Ａ２は記録媒体に記録された形態で配信される。もっとも、常にディジタルデータの配信に先立って行われなければならない訳ではない。暗号処理の解除に必要な鍵がディジタルデータの配信後に行われる場合もあり得る。

【０１７０】

ディジタルデータと合わせ鍵の配信を受けた下流側システムが、所定の出力スケジュールに従ってディジタルデータを読み出し、復元された暗号鍵で暗号処理を解除する。その後、暗号処理の解除されたディジタルデータのうち特定者のシステム構成に適合するコーデック方式にかかるものが選択的に復号化され、復号結果についてのスクランブル処理が復号サーバ３３にて実行される。

【０１７１】

この後、復号サーバ３３からはスクランブル処理が施されたディジタルデータが出力装置３４に出力される。出力装置３４では、スクランブル制御部３６から与えられるデスクランブル鍵によってスクランブル処理の解除が行われ、所望の形態でコンテンツの出力が行われる。なおこの出力状況が出力ログとして出力ログ管理部３７より上流側システムに通知される。ここでの通知は、コンテンツの出力毎に行われても良い（すなわち、１回の出力に付き１回通知されても良い）し、複数回の出力情報をまとめて通知しても良い（例えば、１日毎に出力状況リストを出力しても良い）。

【０１７２】

（２－１－５）第１の配信システム例によって得られる効果

上述のように第１の配信システム例によれば、合わせ鍵の配信経路を複数としたことにより、たとえいずれかの合わせ鍵が盗難されたとしても他方も盗難されない限り暗号鍵の流出を防止できる配信モデルを提供できる。特に、合わせ鍵をディジタルデータとは別の経路（上述のように同一の伝送媒体を用いながら時間的に別の時点に配信する場合を含む。）で配信する場合には、合わせ鍵の一部を盗んだ不正行為者が暗号化されたディジタルデータをも入手した場合でも、暗号鍵の復元に必要な鍵情報はディジタルデータとは別に配信されるため、生のディジタルデータが復号化される事態を確実に回避できる。

【０１７３】

また暗号処理が解除されたディジタルデータにスクランブル処理を施す方式を採用したことにより、不正行為に対する十分な防御能力を保持したままで復号機能を実行するサーバ装置と再生機能を実行する出力装置との分離を実現できる。

【０１７４】

特に、運用後により安全性が高い暗号方式が出現した場合や取り扱うコーデック方式を変更したい場合でも、復号サーバ３３のみを置き換えることで対処できる。また、特定者が取り扱うコーデック方式が何であったとしても、復号サーバ３３から出力装置３４に出力されるデータはスクランブル処理されたデータに統一されるため、出力装置３４を複数のコーディク方式で共用できる。

【０１７５】

このことは出力装置３４の開発費が少なく済むことをも意味する。すなわち、汎用型の出力装置３４にデスクランブル部３４Ａを搭載すると共に、正規な手続きでしか開封できないか又は動作しない仕組みを搭載するだけでよいため、出力装置３４の低価格化を実現できる。従って、運用後により性能の高い出力装置が開発された場合でも、例えば再現解像度の高いものが開発された場合でも、装置の置き換えが進み易い。

【０１７６】

かくして、不正行為に対する安全性もシステムを運用する上での経済性も同時に満足できる。

【０１７７】

（２－２）第２の配信システム例

図５に、上述のビジネスモデルを実現するための第２のシステム例を示す。ここで図５は、図４との対応部分に同一符号を付して表したものである。図５と図４を対比して分かるように、当該システムを構成する下流側システムは第１の配信システム例と同じである。なお第２の配信システム例は前述の第２の手段に対応する。

【０１７８】

（２－２－１）概念構成

まず当該第２の配信システム例の概念構成を説明する。この第２の配信システムの場合も、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０１７９】

（１）第１のモデル

第１のモデルとして見た上流側システムは、各ディジタルデータに固有の暗号鍵を発生する処理と、ディジタルデータを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を第１の伝送網を通じて各特定者に配信する処理と、生成された部分鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報を第２の伝送網を通じて特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。

【０１８０】

一方、下流側システムは、第１の伝送網を通じて配信を受けた部分鍵又はその発生情報と、記録媒体の形態で配信を受けた部分鍵又はその発生情報と、第２の伝送網を通じて配信を受けた合わせ鍵又はその発生情報を基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０１８１】

ここで、合わせ鍵から一組の部分鍵を生成するのに用いる分割規則は、全ての配信先に共通の規則でも良いし、各配信先に固有の規則でも良いし、特定地域その他の条件で区分された配信先の集合毎に固有の規則でも良い。他の手段においても同様である。

【０１８２】

なおここでは、合わせ鍵の一部を更に分割して配信用の鍵情報を生成しているがこれに代え、多重鍵で暗号化する方式を採用することもできる。かかる変形例は、同様の仕組みを採用する他の手段についても同様である。

【０１８３】

（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、第１の伝送網を通じ

て配信を受けた部分鍵又はその発生情報と、記録媒体の形態で配信を受けた部分鍵又はその発生情報と、第２の伝送網を通じて配信を受けた合わせ鍵又はその発生情報を基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理の解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０１８４】

このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。

【０１８５】

（２－２－２）システム構成

本システム例と第１の配信システム例との違いは、合わせ鍵生成部１８で生成された合わせ鍵Ａ１を更に分割する部分鍵生成部２０が追加された点と、当該部分鍵生成部２０で生成された部分鍵を記録媒体に書き込むための書込部２１とその読み取り用の読取部３８が設けられた点と、配信される鍵情報が３つになったことに伴って鍵情報の配信方法に一部変更が生じた点である。

【０１８６】

部分鍵生成部２０は、合わせ鍵生成部１８の分割処理により得られた合わせ鍵の一部Ａ１を所定の分割パターンで分割し、一組の部分鍵Ａ１１及びＡ１２を生成する装置である。例えば、配信先となる特定者が１０００人いれば、１０００組の部分鍵Ａ１１及びＡ１２が生成される。もっとも所定の分割パターンはこのように配信先毎に異なる場合だけでなく、全ての配信先について同じでも良い。

また、特定地域や管理グループ毎に異なっていても良い。

【０１８７】

生成された部分鍵は、部分鍵生成部２０によって配信先管理サーバ１７と所定の配信処理部に与えられる。このシステムの場合、部分鍵生成部２０は、部分鍵Ａ１１をネットワークを介しての配信用に不図示の通信部に与え、残る部分鍵Ａ１２を記録媒体による配信用に書込部２１に与える。

【０１８８】

書込部２１は、通知を受けた部分鍵Ａ１２を所定の記録媒体に書き込むための装置である。書込部２１には、記録媒体に応じた駆動機構が設けられる。記録媒体には、磁気読み取り方式の媒体、光学読み取り方式の媒体、半導体メモリその他の媒体が用いられる。なお、記録媒体の配信に必要な宛先情報は配信先管理サーバ１７から与えられる。前述の不図示の通信部についても同様である。ただし、通信部の場合にはネットワーク上のアドレスが与えられる。

【０１８９】

なお当該書込部２１と対をなす読取部３８には、配信を受ける記録媒体に応じた駆動機構を備えるものが用いられる。

【０１９０】

また、第１の配信システム例では、合わせ鍵生成部１８で生成された合わせ鍵Ａ２は記録媒体を通じて下流側システムに配信されていたが、この第２の配信システム例の場合、合わせ鍵Ａ２はネットワークを介して配信される。

【０１９１】

以上が第２の配信システム例と第１の配信システム例との相違点である。なお基本的なシステム構成については何ら変更がないため、鍵情報の配信動作以外は第１の配信システム例と同様に実行される。

【０１９２】

（２－２－３）第２のシステム例によって得られる効果

以上のように第２の配信システム例によれば、鍵情報の配信を２つの伝送網（異なる伝送網を用いる場合と、同一伝送網に異なる時点で鍵情報を配信する場合とがある。）と記録媒体とで実現するため、すなわち第１のシステムよりも更に

鍵情報の配信経路が増えるため、伝送経路上での不正行為がより困難なものを提供できる。

【０１９３】

（２－３）第３の配信システム例

図６に、上述のビジネスモデルを実現するための第３の配信システム例を示す。ここで図６は、図４及び図５との対応部分に同一符号を付して表したものである。なお第３の配信システム例は前述の第２の手段に対応する。

【０１９４】

（２－３－１）概念構成

まず当該第３の配信システム例の概念構成を説明する。この第３の配信システムの場合も、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０１９５】

（１）第１のモデル

第１のモデルとして見た上流側システムは、各ディジタルデータに固有の暗号鍵を発生する処理と、ディジタルデータを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を伝送網を通じて各特定者に配信する処理と、残りの部分鍵又はその発生情報を記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報を記録媒体の形態での配信用に鍵専用の第２の記録媒体に記録する処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。

【０１９６】

一方、下流側システムは、第１の伝送網を通じて配信を受けた部分鍵又はその発生情報と、記録媒体の形態で配信を受けた残りの部分鍵又はその発生情報と、第２の記録媒体の形態で配信を受けた合わせ鍵又はその発生情報を基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対

応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０１９７】

（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、第１の伝送網を通じて配信を受けた部分鍵又はその発生情報と、第２の記録媒体の形態で配信を受けた残りの部分鍵又はその発生情報と、記録媒体の形態で配信を受けた合わせ鍵又はその発生情報を基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０１９８】

このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。

【０１９９】

（２－３－２）システム構成

本システム例における上流側システムと第２の配信システム例との違いは、合わせ鍵Ａ２の配信がネットワークを介して行われるのではなく、第１の配信システム例のように記録媒体を通じて実現される点である。このため、合わせ鍵Ａ２の配信経路については、第１の配信システム例と同じものが用いられている。

【０２００】

以上が第３の配信システムと上述した配信システム例との相違点である。なお

基本的なシステム構成については何ら変更がないため、鍵情報の配信動作以外は第１の配信システムや第２の配信システムと同様である。

【０２０１】

（２－３－３）第３の配信システム例によって得られる効果

以上のように第３の配信システム例によれば、鍵情報の配信を１つの伝送網と２つの記録媒体とで実現するため、すなわち第２の配信システム例よりも記録媒体による配信経路が増えるため、鍵情報の盗難を発見し易いより不正行為に対する安全性の高いものを提供できる。

【０２０２】

（２－４）第４の配信システム例

図７に、上述のビジネスモデルを実現するための第４の配信システム例を示す。ここで図７は、図４との対応部分に同一符号を付して表したものである。なお第４の配信システム例は前述の第１の手段に対応する。

【０２０３】

（２－４－１）概念構成

まず当該第４の配信システム例の概念構成を説明する。この第４の配信システムの場合も、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０２０４】

（１）第１のモデル

第１のモデルとして見た上流側システムは、各ディジタルデータに固有の暗号鍵を発生する処理と、ディジタルデータを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部を第１の伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵又はその発生情報のうち残りの部分を第２の伝送網を通じて各特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。

【０２０５】

一方、下流側システムは、第１の伝送網を通じて配信を受けた合わせ鍵又はそ

の発生情報の一部と、第２の伝送網を通じて配信を受けたそれらと対をなす残りの部分とを基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０２０６】

（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、第１の伝送網を通じて配信を受けた合わせ鍵又はその発生情報の一部と、第２の伝送網を通じて配信を受けたそれらと対をなす残りの部分とを基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理において生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０２０７】

このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。

【０２０８】

（２－４－２）システム構成

本システム例における上流側システムと第１の配信システム例との違いは、合わせ鍵生成部１８で発生された合わせ鍵Ａ１及びＡ２がいずれもネットワークを介して配信される点である。

【０２０９】

以上が第４の配信システムと第１の配信システム例との相違点である。なお基本的なシステム構成については何ら変更がないため、鍵情報の配信動作以外は第１の配信システム例と同様である。

【０２１０】

（２－４－３）第４の配信システム例によって得られる効果

以上のように第４の配信システム例によれば、鍵情報の配信を２つともネットワークを介して実現するため、すなわち全ての鍵情報を即時性に優れたネットワークを通じて配信できるため、記録媒体を使用して鍵情報の配信を行う場合と比べ、鍵の配信からディジタルデータの配信が開始されるまでの時間を大幅に短縮できる。

【０２１１】

（２－５）第５の配信システム例

図８に、上述のビジネスモデルを実現するための第５の配信システム例を示す。ここで図８は、図４との対応部分に同一符号を付して表したものである。なお第５の配信システム例は前述の第１の手段に対応する。

【０２１２】

（２－５－１）概念構成

まず当該第５の配信システム例の概念構成を説明する。この第５の配信システムの場合も、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０２１３】

（１）第１のモデル

第１のモデルとして見た上流側システムは、各ディジタルデータに固有の暗号鍵を発生する処理と、ディジタルデータを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部を記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、生成された合わせ鍵又はその発生情報のうち残りの部分を記録媒体の形態での配信用に鍵専用の第２の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配

信する処理とを実行する。

【０２１４】

一方、下流側システムは、第１の記録媒体の形態で配信を受けた合わせ鍵又はその発生情報の一部と、第２の記録媒体の形態で配信を受けたそれらと対をなす残りの部分とを基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０２１５】

（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、第１の記録媒体の形態で配信を受けた合わせ鍵又はその発生情報の一部と、第２の記録媒体の形態で配信を受けたそれらと対をなす残りの部分とを基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０２１６】

このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。

【０２１７】

（２－５－２）システム構成

本システム例における上流側システムと第１の配信システム例との違いは、合

わせ鍵生成部１８で発生された合わせ鍵Ａ１及びＡ２がいずれも記録媒体を介して配信される点である。このため、本システムでは、合わせ鍵Ａ１を記録媒体に書き込むための書込部２２と、これと対をなす読取部３９とが新たに設けられている。書込部２２や読取部３９の構成は、他の書込部や読取部の構成と同じである。

【０２１８】

以上が第５の配信システム例と第１の配信システム例との相違点である。なお基本的なシステム構成については何ら変更がないため、鍵情報の配信動作以外は第１の配信システムと同様である。

【０２１９】

（２－５－３）第５の配信システム例によって得られる効果

以上のように第５の配信システム例によれば、鍵情報の配信を２つとも記録媒体を介して実現するため、すなわち全ての鍵情報を盗難の発見が容易な記録媒体を通じて配信できるため、ネットワークを介して鍵情報を配信する場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【０２２０】

（２－６）第６の配信システム例

図９に、上述のビジネスモデルを実現するための第６の配信システム例を示す。ここで図９は、図５との対応部分に同一符号を付して表したものである。なお第６の配信システム例は前述の第２の手段に対応する。

【０２２１】

（２－６－１）概念構成

まず当該第６の配信システム例の概念構成を説明する。この第６の配信システムの場合も、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０２２２】

（１）第１のモデル

第１のモデルとして見た上流側システムは、各ディジタルデータに固有の暗号鍵を発生する処理と、ディジタルデータを対応する暗号鍵で暗号化する処理と、

暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を第１の伝送網を通じて各特定者に配信する処理と、残る部分鍵又はその発生情報を第２の伝送網を通じて各特定者に配信する処理と、部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報を第３の伝送網を通じて各特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。る。

【０２２３】

一方、下流側システムは、第１の伝送網を通じて配信を受けた部分鍵又はその発生情報と、第２の伝送網を通じて配信を受けた残りの部分鍵又はその発生情報と、第３の伝送網を通じて配信を受けた合わせ鍵又はその発生情報を基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０２２４】

（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、第１の伝送網を通じて配信を受けた部分鍵又はその発生情報と、第２の伝送網を通じて配信を受けた残りの部分鍵又はその発生情報と、第３の伝送網を通じて配信を受けた合わせ鍵又はその発生情報を基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０２２５】

このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。

【０２２６】

（２－６－２）システム構成

本システム例における上流側システムと第２の配信システム例（図５）との違いは、部分鍵生成部２０で発生された部分鍵Ａ１２がネットワークを介して配信される点である。

【０２２７】

以上が第６の配信システム例と第２の配信システム例との相違点である。なお基本的なシステム構成については何ら変更がないため、鍵情報の配信動作以外は第２の配信システムと同様である。

【０２２８】

（２－６－３）第６の配信システム例によって得られる効果

以上のように第６の配信システム例によれば、鍵情報の配信を３つともネットワークを介して実現するため、すなわち全ての鍵情報を即時性に優れたネットワークを通じて配信できるため、記録媒体を使用して鍵情報の配信を行う場合と比べ、鍵の配信からディジタルデータの配信が開始されるまでの時間を大幅に短縮できる。

【０２２９】

更に、配信される鍵情報の数が３つであるため、２つの鍵情報をネットワークを介して鍵情報を配信する場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【０２３０】

（２－７）第７の配信システム例

図１０に、上述のビジネスモデルを実現するための第７の配信システム例を示

す。ここで図１０は、図６及び図８との対応部分に同一符号を付して表したものである。なお第７の配信システム例は前述の第２の手段に対応する。

【０２３１】

（２－７－１）概念構成

まず当該第７の配信システム例の概念構成を説明する。この第７の配信システムの場合も、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０２３２】

（１）第１のモデル

第１のモデルとして見た上流側システムは、各ディジタルデータに固有の暗号鍵を発生する処理と、ディジタルデータを対応する暗号鍵で暗号化する処理と、暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵又はその発生情報の一部について更に複数の部分鍵を生成する処理と、生成された部分鍵の一部又はその発生情報を記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、残りの部分鍵又はその発生情報を記録媒体の形態での配信用に鍵専用の第２の記録媒体に書き込む処理と、部分鍵の生成に用いなかった残りの合わせ鍵又はその発生情報を記録媒体の形態での配信用に鍵専用の第３の記録媒体に記録する処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。

【０２３３】

一方、下流側システムは、第１の記録媒体の形態で配信を受けた部分鍵又はその発生情報と、第２の記録媒体の形態で配信を受けた残りの部分鍵又はその発生情報と、第３の記録媒体の形態で配信を受けた合わせ鍵又はその発生情報とを基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０２３４】

（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、第１の記録媒体の形

態で配信を受けた部分鍵又はその発生情報と、第２の記録媒体の形態で配信を受けた残りの部分鍵又はその発生情報と、第３の記録媒体の形態で配信を受けた合わせ鍵又はその発生情報とを基に対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０２３５】

このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。

【０２３６】

（２－７－２）システム構成

本システム例における上流側システムと第３の配信システム例との違いは、部分鍵生成部２０で発生された部分鍵Ａ１１及びＡ１２がいずれも記録媒体を介して配信される点である。このため、本システム例では、部分鍵Ａ１１を記録媒体に書き込むための書込部２２と、これと対をなす読取部３９とが新たに設けられている。書込部２２や読取部３９の構成は、他の書込部や読取部の構成と同じである。

【０２３７】

以上が第７の配信システム例と第３の配信システム例との相違点である。なお基本的なシステム構成については何ら変更がないため、鍵情報の配信動作以外は第３の配信システムと同様である。

【０２３８】

（２－７－３）第７の配信システム例によって得られる効果

以上のように第７の配信システム例によれば、鍵情報の配信を３つとも記録媒体を介して実現するため、すなわち全ての鍵情報を盗難の発見が容易な記録媒体を通じて配信できるため、ネットワークを介して鍵情報を配信する経路を含む場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【０２３９】

（２－８）第８の配信システム例

図１１に、上述のビジネスモデルを実現するための第８の配信システム例を示す。ここで図１１は、図４との対応部分に同一符号を付して表したものである。当該システム例は、前述までの第１～第７の配信システム例とは異なり、ディジタルデータの暗号鍵を分割するのではなく、当該暗号鍵を配信先毎に固有の別の多重鍵で暗号化するものである。すなわち第８の配信システム例は前述の第３の手段に対応するものである。

【０２４０】

（２－８－１）概念構成

まず当該第８の配信システム例の概念構成を説明する。この第８の配信システムの場合も、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０２４１】

（１）第１のモデル

第１のモデルとして見た上流側システムは、各ディジタルデータに固有の第１の暗号鍵を発生する処理と、ディジタルデータを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルデータに固有のものを発生する処理と、第２の暗号鍵によって第１の暗号鍵又はその発生情報を暗号化し、伝送網を通じて特定者に配信する処理と、第２の暗号鍵を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。

【０２４２】

一方、下流側システムは、記録媒体の形態で配信を受けた第２の暗号鍵又はその発生情報を基に、伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除して、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０２４３】

（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、記録媒体の形態で配信を受けた第２の暗号鍵又はその発生情報を基に、伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除して、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０２４４】

このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。

【０２４５】

（２－８－２）システム構成

前述のように、第８の配信システム例は前述の第１～第７の配信システム例とは基本な処理方式を異にする。このため第８の配信システム例では、配信先に固有の多重鍵Ｂを生成する多重鍵生成部２３と、当該多重鍵Ｂによって暗号鍵Ａを

暗号化する鍵暗号化処理部２４と、多重鍵Ｂを記録媒体に書き込んで配信するのに使用する書込部２５と、これと対をなす読取部４０を、第１の配信システム例における合わせ鍵生成部１８、書込部１９、読取部３２に置き換えて使用する。

【０２４６】

多重鍵生成部２３は、コンテンツ毎に生成された暗号鍵Ａに配信先毎に固有の暗号鍵Ｂを生成する装置である。例えば、配信先となる特定者が１０００人いれば、１０００通りの多重鍵Ｂを生成する。なお多重鍵Ｂは、配信先が同じであれば常に同じ多重鍵を用いる方法もあれば、コンテンツ毎に異なる多重鍵Ｂを生成して用いる場合もある。安全性の観点からは後者が望ましい。また、特定地域や管理グループ毎に異なる鍵を使っても良い。

【０２４７】

鍵暗号化処理部２４は、配信先毎に固有の多重鍵を用いて暗号鍵を暗号化する装置である。鍵暗号化処理部２４で暗号化された暗号鍵は、不図示の通信部よりネットワークを介して対応する下流側システムに配信される。

【０２４８】

書込部２５と読取部４０の構成は上述の書込部及び読取部と同じである。もっとも、書込部２５と読取部４０によって読み書きされるのは多重鍵である点で上述の配信システム例とは異なる。

【０２４９】

（２－８－３）ディジタルデータの配信動作

第８の配信システム例におけるディジタルデータの配信動作のうち第１の配信システム例と異なる部分についてのみ簡単に説明する。すなわち、第１の配信システム例では、コンテンツに固有の暗号鍵Ａを発生すると当該暗号鍵を合わせ鍵生成部１８に与えて合わせ鍵を生成したが、本システム例の場合、配信先毎に発生された固有の多重鍵Ｂを用いて暗号鍵Ａを暗号化し、ネットワークを介して下流側システムに配信する。また、当該暗号鍵Ａの暗号化に使用した多重鍵Ｂをそれぞれ対応する配信者に宛てて記録媒体の形態で配信する。

【０２５０】

なお生成された多重鍵Ｂは、配信先管理サーバ１７にて管理される。以上の処

理動作が第１のシステムとの主な違いである。

【０２５１】

（２－８－４）第８の配信システム例によって得られる効果

上述のように第８の配信システム例によれば、下流側システムを管理する特定者に配信する鍵情報を暗号化された暗号鍵Ａと多重鍵Ｂとの２つとし、それらを複数の経路を介して配信する構成としたことにより、たとえいずれかの鍵情報が盗難されたとしても他方も盗難されない限り暗号鍵の流出を防止できる配信モデルを提供できる。

【０２５２】

しかも多重鍵については盗難を発見し易い記録媒体の形態で配信を行うため、不正行為によって多重鍵が盗難されたことが明らかになった場合にはネットワークを介して行う暗号化された暗号鍵Ａの配信を行うのを中止し、別の多重鍵Ｂを記録媒体として配信する手順から再開することで不正行為に対する安全性を保つことができる。

【０２５３】

勿論、下流側システムの構成は第１の配信システム例と同じであるため、運用に際しての経済性にも優れることは第１の配信システム例と同様である。

【０２５４】

（２－９）第９の配信システム例

図１２に、上述のビジネスモデルを実現するための第９のシステム例を示す。ここで図１２は、図１１との対応部分に同一符号を付して表したものである。なお第９の配信システム例は前述の第４の手段に対応する。

【０２５５】

（２－９－１）概念構成

まず当該第９の配信システム例の概念構成を説明する。この第９の配信システムの場合も、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０２５６】

第１のモデルとして見た上流側システムは、各ディジタルデータに固有の第１

の暗号鍵を発生する処理と、ディジタルデータを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルデータに固有のものを発生する処理と、上記第２の暗号鍵によって第１の暗号鍵又はその発生情報を暗号化し、第１の伝送網を通じて特定者に配信する処理と、第２の暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を第２の伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。

【０２５７】

一方、下流側システムは、第２の伝送網を通じて配信を受けた合わせ鍵の一部と、記録媒体を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０２５８】

（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、第２の伝送網を通じて配信を受けた合わせ鍵の一部と、記録媒体を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスク

ランブル処理して出力する処理とを実行する。

【０２５９】

このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。

【０２６０】

（２－９－２）システム構成

本システム例と第８の配信システム例との違いは、多重鍵生成部２３で生成された多重鍵Ｂを分割し、一組の合わせ鍵Ｂ１とＢ２を生成する合わせ鍵生成部２６が追加された点と、当該合わせ鍵生成部２６で生成された合わせ鍵の一部Ｂ２を記録媒体に書き込むための書込部２７とその読み取り用の読取部４１が設けられた点である。

【０２６１】

合わせ鍵生成部２６は、配信先毎に生成された多重鍵Ｂを配信先毎に固有の分割パターンで分割し、一組の合わせ鍵Ｂ１及びＢ２を生成する装置である。合わせ鍵生成部２６の分割規則は、全ての配信先について共通の分割規則を用いることも可能であるし、配信先毎に固有の分割規則を割り当てることも可能であるし、これら分割規則をコンテンツ単位で変更することも可能である。またコンテンツの配信中も定期又は不定期に変更することも可能である。また特定地域や管理グループ毎に異なる分割規則を割り当てることも可能である。

【０２６２】

書込部２７と読取部４１の構成は他の書込部や読取部と同じである。なお基本的なシステム構成については何ら変更がないため、鍵情報の配信動作以外は第８の配信システム例と同様である。

【０２６３】

（２－９－３）第９の配信システム例によって得られる効果

以上のように第９の配信システム例によれば、多重鍵Ｂを一組の合わせ鍵Ｂ１

及びＢ２に分割して一方をネットワークで、他方を記録媒体で配信する構成を採用するため、すなわち多重鍵Ｂそのものを送るのでなく分割したものを配信するのに加え、配信経路を２つから３つに増やすことにより、第８の配信システム例に比べてより不正行為に対する安全性の高いものを提供できる。

【０２６４】

（２－１０）第１０の配信システム例

図１３に、上述のビジネスモデルを実現するための第１０の配信システム例を示す。ここで図１３は、図１２との対応部分に同一符号を付して表したものである。なお第１０の配信システム例は前述の第４の手段に対応する。

【０２６５】

（２－１０－１）概念構成

まず当該第１０の配信システム例の概念構成を説明する。この第１０の配信システムには、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０２６６】

（１）第１のモデル

第１のモデルとして見た上流側システムは、各ディジタルデータに固有の第１の暗号鍵を発生する処理と、ディジタルデータを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルデータに固有のものを発生する処理と、第２の暗号鍵によって暗号化された第１の暗号鍵又はその発生情報を、記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、第２の暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を伝送網を通じて各特定者に配信する処理と、生成された合わせ鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の第２の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。

【０２６７】

一方、下流側システムは、伝送網を通じて配信を受けた合わせ鍵の一部と、第

２の記録媒体を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の記録媒体を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０２６８】

（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、伝送網を通じて配信を受けた合わせ鍵の一部と、第２の記録媒体を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の記録媒体を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先であって、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０２６９】

このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。

【０２７０】

（２－１０－２）システム構成

本システム例と第９の配信システム例との違いは、暗号化された暗号鍵Ａの配信をネットワークを介して行うのではなく、記録媒体を介して行う点である。こ

のため、本システム例の場合には、書込部２８と読取部４２が新たに設けられる点で異なっている。書込部２８と読取部４２の構成は他の書込部や読取部と同じであるため省略する。

【０２７１】

なお基本的なシステム構成については何ら変更がないため、鍵情報の配信動作以外は第８の配信システム例と同様である。

【０２７２】

（２－１０－３）第１０の配信システム例によって得られる効果

以上のように第１０の配信システム例によれば、暗号化された暗号鍵Ａが記録媒体を通じて配信される分、当該鍵がネットワークを介して配信される場合に比して盗難の早期発見が可能となり、暗号鍵の変更等の対策を採り易いという効果を期待できる。

【０２７３】

（２－１１）第１１の配信システム例

図１４に、上述のビジネスモデルを実現するための第１１の配信システム例を示す。ここで図１４は、図１１との対応部分に同一符号を付して表したものである。なお第１１の配信システム例は前述の第３の手段に対応する。

【０２７４】

（２－１１－１）概念構成

まず当該第１１の配信システム例の概念構成を説明する。この第１１の配信システムには、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０２７５】

（１）第１のモデル

第１のモデルとして見た上流側システムは、各ディジタルデータに固有の第１の暗号鍵を発生する処理と、ディジタルデータを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルデータに固有のものを発生する処理と、第２の暗号鍵によって第１の暗号鍵又はその発生情報を暗号化し、第１の伝送網を通じて特定者に配信する処理と、第２の暗号鍵

を第２の伝送網を通じて特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。

【０２７６】

一方、下流側システムは、第２の伝送網を通じて配信を受けた第２の暗号鍵又はその発生情報を基に、第１の伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０２７７】

（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、第２の伝送網を通じて配信を受けた第２の暗号鍵又はその発生情報を基に、第１の伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０２７８】

このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。

【０２７９】

（２－１１－２）システム構成

本システム例と第８の配信システム例との違いは、多重鍵Ｂを記録媒体を介して行うのではなく、ネットワークを介して行う点である。それ以外は第８の配信システム例と同じであるため、鍵情報の配信動作以外は第８の配信システム例と同様である。もっとも、多重鍵Ｂの配信に際しては、電子証明書等で相手方の正当性を確認した上で、配信先が公開している公開鍵で暗号化して配信するのが望ましい。

【０２８０】

（２－１１－３）第１１の配信システム例によって得られる効果

以上のように第１１の配信システム例によれば、多重鍵Ｂをネットワークを介して配信する手法を採用するため、鍵の配信からディジタルデータの配信が開始されるまでの時間を大幅に短縮できる。

【０２８１】

（２－１２）第１２の配信システム例

図１５に、上述のビジネスモデルを実現するための第１２の配信システム例を示す。ここで図１５は、図１１及び図１３との対応部分に同一符号を付して表したものである。なお第１２の配信システム例は前述の第３の手段に対応する。

【０２８２】

（２－１２－１）概念構成

まず当該第１２の配信システム例の概念構成を説明する。この第１２の配信システムには、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０２８３】

（１）第１のモデル

第１のモデルとして見た上流側システムは、各ディジタルデータに固有の第１の暗号鍵を発生する処理と、ディジタルデータを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルデータに固有のものを発生する処理と、第２の暗号鍵によって第１の暗号鍵又はその発生情報を暗号化し、記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、第２の暗号鍵を記録媒体の形態での配信用に鍵専用の第２の記録媒体

に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。

【０２８４】

一方、下流側システムは、第２の記録媒体の形態で配信を受けた第２の暗号鍵又はその発生情報を基に、第１の記録媒体の形態で配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０２８５】

（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、第２の記録媒体の形態で配信を受けた第２の暗号鍵又はその発生情報を基に、第１の記録媒体の形態で配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０２８６】

このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。

【０２８７】

（２－１２－２）システム構成

本システム例と第８の配信システム例との違いは、暗号化された暗号鍵Ａの配信をネットワークを介して行うのではなく、記録媒体を介して行う点である。それ以外は第８の配信システム例と同じであるため、鍵情報の配信動作以外は第８の配信システム例と同様である。

【０２８８】

（２－１２－３）第１２の配信システム例によって得られる効果

以上のように第１２の配信システム例によれば、鍵情報の配信を２つとも記録媒体を介して実現するため、すなわち全ての鍵情報を盗難の発見が容易な記録媒体を通じて配信できるため、ネットワークを介して鍵情報を配信する場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【０２８９】

（２－１３）第１３の配信システム例

図１６に、上述のビジネスモデルを実現するための第１３の配信システム例を示す。ここで図１６は、図１２との対応部分に同一符号を付して表したものである。なお第１３の配信システム例は前述の第４の手段に対応する。

【０２９０】

（２－１３－１）概念構成

まず当該第１３の配信システム例の概念構成を説明する。この第１３の配信システムには、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０２９１】

（１）第１のモデル

第１のモデルとして見た上流側システムは、システム内の何処かに、各ディジタルデータに固有の第１の暗号鍵を発生する処理と、ディジタルデータを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルデータに固有のものを発生する処理と、第２の暗号鍵によって第１の暗号鍵又はその発生情報を暗号化し、第１の伝送網を通じて特定者に配信する処理と、第２の暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を第２の伝送網を

通じて各特定者に配信する処理と、生成された合わせ鍵の残りの部分又はその発生情報を第３の伝送網を通じて各特定者に配信する処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。

【０２９２】

一方、下流側システムは、第２の伝送網を通じて配信を受けた合わせ鍵の一部と、第３の伝送網を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０２９３】

（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、第２の伝送網を通じて配信を受けた合わせ鍵の一部と、第３の伝送網を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の伝送網を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０２９４】

このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力

形態で出力する処理とを実行する。

【０２９５】

（２－１３－２）システム構成

本システム例と第９の配信システム例との違いは、多重鍵Ｂから生成した合わせ鍵Ｂ２の配信に記録媒体を用いるのではなく、ネットワークを介して行う点である。すなわち、３つの鍵情報の配信を全てネットワークを介して行う点で異なっている。それ以外は第９の配信システム例と同じであるため、鍵情報の配信動作以外は第９の配信システム例と同様である。

【０２９６】

（２－１３－３）第１３の配信システム例によって得られる効果

以上のように第１３の配信システム例によれば、鍵情報の配信を３つともネットワークを介して行うため、記録媒体を使用して鍵情報の配信を行う場合と比べ、鍵の配信からディジタルデータの配信が開始されるまでの時間を大幅に短縮できる。

【０２９７】

更に、配信される鍵情報の数が３つであるため、２つの鍵情報をネットワークを介して鍵情報を配信する場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【０２９８】

（２－１４）第１４のシステム例

図１７に、上述のビジネスモデルを実現するための第１４の配信システム例を示す。ここで図１７は、図１３との対応部分に同一符号を付して表したものである。なお第１４の配信システム例は前述の第４の手段に対応する。

【０２９９】

（２－１４－１）概念構成

まず当該第１４の配信システム例の概念構成を説明する。この第１４の配信システムには、ディジタルデータの配信に着目した第１のモデルと、ディジタルデータの受け手側に着目した第２のモデルとが含まれる。

【０３００】

（１）第１のモデル

第１のモデルとして見た上流側システムは、各ディジタルデータに固有の第１の暗号鍵を発生する処理と、ディジタルデータを第１の暗号鍵で暗号化する処理と、配信先である各特定者に固有の第２の暗号鍵であって、ディジタルデータに固有のものを発生する処理と、第２の暗号鍵によって暗号化された第１の暗号鍵又はその発生情報を、記録媒体の形態での配信用に鍵専用の第１の記録媒体に書き込む処理と、第２の暗号鍵を基に配信先である各特定者に固有の一組の合わせ鍵を生成する処理と、生成された合わせ鍵の一部又はその発生情報を記録媒体の形態での配信用に鍵専用の第２の記録媒体に書き込む処理と、生成された合わせ鍵の残りの部分又はその発生情報を記録媒体の形態での配信用に鍵専用の第３の記録媒体に書き込む処理と、配信スケジュールに従って暗号処理の施されたディジタルデータを配信する処理とを実行する。

【０３０１】

一方、下流側システムは、第２の記録媒体を通じて配信を受けた合わせ鍵の一部と、第３の記録媒体を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の記録媒体を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理とを実行する。

【０３０２】

（２）第２のモデル

第２のモデルとして見た下流側システムの復号サーバは、第２の記録媒体を通じて配信を受けた合わせ鍵の一部と、第３の記録媒体を通じて配信を受けた合わせ鍵の残りの部分とから第２の暗号鍵を復元して、第１の記録媒体を通じて配信を受けた第１の暗号鍵又はその発生情報に施されている暗号処理を解除し、対応するディジタルデータに固有の暗号鍵を復元する処理と、復元された暗号鍵を用い対応するディジタルデータに施されている暗号処理を解除する処理と、ディジタルデータに付属する再生条件が満たされることを条件にスクランブル鍵とその解除鍵とを局所的に生成する処理と、暗号処理が解除されたディジタルデータの

唯一の出力先において、当該ディジタルデータに施されている符号化処理を復号化し、ディジタルデータを復元する処理と、復元されたディジタルデータの唯一の出力先において、上記処理で生成されたスクランブル鍵を用い、ディジタルデータをスクランブル処理して出力する処理とを実行する。

【０３０３】

このとき下流側システムの出力装置は、復号サーバから入力されるディジタルデータに施されているスクランブル処理を、復号サーバから与えられたスクランブル解除鍵によって解除する処理と、上記処理でスクランブル処理が解除されたディジタルデータの唯一の出力先において、当該ディジタルデータを所定の出力形態で出力する処理とを実行する。

【０３０４】

（２－１４－２）システム構成

本システム例と第１０の配信システム例との違いは、多重鍵Ｂから生成した合わせ鍵Ｂ１の配信にネットワークを用いるのではなく、記録媒体を介して行う点である。すなわち、３つの鍵情報の配信を全て記録媒体を介して行う点で異なっている。このため、本システム例の場合には、書込部２９と読取部４３が新たに設けられている。書込部２９と読取部４３の構成は他の書込部や読取部と同じであるため省略する。

【０３０５】

それ以外は第１０の配信システム例と同じであるため、鍵情報の配信動作以外は第１０の配信システム例と同様である。

【０３０６】

（２－１４－３）第１４の配信システム例によって得られる効果

以上のように第１４の配信システム例によれば、鍵情報の配信を３つとも記録媒体を介して行うため、すなわち全ての鍵情報を盗難の発見が容易な記録媒体を通じて配信できるため、ネットワークを介して鍵情報を配信する経路を含む場合と比べ、より不正行為に対する安全性の高いものを提供できる。

【０３０７】

（３）各システム例で想定される運用形態

第１～第１４の配信システム例では、上流側システムを構成する機能部のいずれが配信権者１のシステム内で行われ、いずれが電子配信事業者２のシステム内で行われるか問題とすることなく（上流側システムが３者以上で運用される場合にはそのいずれかで行われるかを問題とすることなく）、当該システム構成から認められる技術的な効果の観点で説明を行ったが、ここでは想定される運用形態についてビジネス上の効果にどのような差異が生じるかについて説明する。

【０３０８】

ここでは特に配給権者から見た上流側システムの安全性について説明する。これは多くの場合、コンテンツの配給権者が不正行為により被害を受けると考えるためであるが、ビジネスモデルによっては他の事業者から見た安全性が優先される可能性があることは言うまでもない。

【０３０９】

図１８は、上流側システムを構成する機能部のうち、コンテンツ符号化部１２と、暗号化部１３と、鍵発生部１６（間接的には合わせ鍵生成部（部分鍵生成部）や多重鍵生成部（その合わせ鍵生成部））がどのように配置されるかの観点からまとめたものである。ただし、図１８では、配信される鍵情報が２種類の場合について示されている。３種類以上の鍵情報が配信される場合には、図１８に「１つ」と表記された箇所は、「少なくとも１つ」を意味する。

【０３１０】

（３－１）第１の運用形態

第１の運用形態では、暗号鍵Ａの発生者、符号化処理の実行者、暗号処理の実行者のいずれもが配給権者である場合（すなわち、コンテンツ符号化部１２、暗号化部１３、鍵発生部１６が配給権者のシステム側に設けられる場合）であって、鍵情報の配信も配給権者が行う場合を考える。

【０３１１】

ここで、鍵情報の発生は配給主体である配給権者が行う場合を想定する。すなわち、合わせ鍵生成部１８（システム例によっては部分鍵生成部２０も含む。）や多重鍵生成部２３及び鍵暗号化処理部２４（システム例によっては合わせ鍵生成部２６も含む。）も配給権者が行う場合を想定する。

【０３１２】

この場合、電子配信事業者２のシステムは暗号処理の施されたディジタルデータを特定者に配信するだけの業務を行うことになる。すなわち、送出サーバ１４のみが電子配信事業者２のシステムに属することになる。

【０３１３】

このような運用形態を採ると、ディジタルデータの暗号化に使用した暗号鍵（マスター鍵）を知り得る立場にある者は配給権者１のみとできる。このことは、配給権者１からみると、電子配信事業者２を通じて暗号鍵が外部に流出する危険性を一切考慮しなくて済むため、安心してコンテンツの提供を行えるという利点がある。

【０３１４】

（３－２）第２の運用形態

第２の運用形態では、基本的には第１の運用形態の下に、鍵情報の配信主体が配給権者１と電子配信事業者２の２者となる場合を考える。

【０３１５】

例えば、第２の配信システム例（図５）において合わせ鍵Ａ２の生成と配信は配給権者１が行うが、合わせ鍵Ａ１から部分鍵Ａ１１とＡ１２を生成する処理と生成された部分鍵の配信は電子配信事業者２が行う場合が考えられる。この他同様の場合に、第３の配信システム例（図６）、第６の配信システム例（図９）、第７の配信システム例（図１０）が考えられる。

【０３１６】

また例えば、生成された合わせ鍵や部分鍵の記録媒体への書込みと配信のみを電子配信事業者２に実行させる場合も考えられる。かかる場合には、第１の配信システム例（図４）、第２の配信システム例（図５）、第３の配信システム例（図６において部分鍵Ａ１２及び又は合わせ鍵Ａ２を書き込む場合）、第５の配信システム例（図８で合わせ鍵Ａ１又はＡ２を書き込む場合）、第７の配信システム例（図１０でいずれか１つの鍵情報又はいずれか２つの鍵情報を書き込む場合）、第９の配信システム例（図１２で合わせ鍵Ｂ２を書き込む場合）、第１０の配信システム例（図１３で暗号化された暗号鍵又は合わせ鍵Ｂ２を書き込む場合

）、第１２の配信システム例（図１５で暗号化された暗号鍵を書き込む場合）、第１４の配信システム例（図１７でいずれか１つの鍵情報又はいずれか２つの鍵情報を書き込む場合）がある。

【０３１７】

このような運用形態としても、ディジタルデータの暗号化に使用した暗号鍵（マスター鍵）を知り得る立場にある者はコンテンツの配給権者のみとなるため、配給権者にとって安全な運用形態とできる。

【０３１８】

なお以上のものに比べるとやや信頼性は低下するが、既存の配信モデルに比して安全性の確保できるものに、第９の配信システム例（図１２）において暗号鍵Ａの暗号化と配信は配給権者１が行うが、多重鍵Ｂの合わせ鍵Ｂ１、Ｂ２の生成と生成された合わせ鍵の配信は電子配信事業者２が行う場合が考えられる。

【０３１９】

これと同様のものに第１０の配信システム例（図１３）、第１２の配信システム例（図１５）、第１３の配信システム例（図１６）、第１４の配信システム例（図１７）が考えられる。

【０３２０】

（３－３）第３の運用形態

第３の運用形態では、基本的には第１の運用形態の下に、鍵情報の配信主体が電子配信事業者２となる場合を考える。

【０３２１】

例えば、第１の配信システム例（図４）において、暗号鍵の発生は配給権者が行うが、発生された暗号鍵を入手して合わせ鍵Ａ１、Ａ２を生成する処理は電子配信事業者２が行う場合が考えられる。これはいずれのシステム例の場合にも考えられる。かかる運用形態を採る場合でも既存の配信モデルに比してシステムの安全性を確保できる。

【０３２２】

（３－４）第４～第６の運用形態

これらの運用形態では、第１～第３の運用形態と異なり、暗号化処理を電子配

信事業者２が実行する場合を考える。すなわち、電子配信事業者２が暗号鍵を配給権者１から入手して暗号処理を実行する場合である。なお、これらの例では符号化処理は配給権者１側が実行するものとする。

【０３２３】

これらの場合では、鍵情報の配信主体が配給権者１のみであるか、電子配信事業者２のみであるか、その両者であるかによらず、結局のところ暗号鍵を知り得る立場にある者がコンテンツ制作会社１と電子配信事業者２の２者となる。ただし、この場合にも既存の配信モデルに比してシステムの安全性を確保できる。

【０３２４】

（３－５）第７～第９の運用形態

これらの運用形態では、第４～第６の運用形態に更に加えて、符号化処理の実行も電子配信事業者２が行う場合を考える。これらの運用形態では、配信権者１はもはや暗号鍵を生成しているだけにすぎず、鍵情報の配信主体が配信権者１のみであるか、電子配信事業者２のみであるか、その両者であるかによらず、結局のところ暗号鍵を知り得る立場にある者が配信権者１と電子配信事業者２の２者となる。ただし、この場合にも既存の配信モデルに比してシステムの安全性を確保できる。

【０３２５】

（３－６）第１０～第１２の運用形態

これらの運用形態では、暗号鍵の生成を電子配信事業者２が行って、ディジタルデータの暗号化は電子配信事業者２から暗号鍵の通知を受けた配信権者１が実施する場合を考える。この場合も、鍵情報の配信主体に誰がなるかにかかわらず、結局のところ暗号鍵を知り得る立場にある者は配信権者１と電子配信事業者２の２者となる。ただし、この場合にも既存の配信モデルに比してシステムの安全性を確保できる。

【０３２６】

（３－７）第１３～第１８の運用形態

これらのうち第１３～第１５の運用形態は、暗号鍵の生成と暗号化処理を電子配信事業者２が実施し、符号化処理のみを配給権者が行う場合である。また第１

６～第１８の運用形態は、暗号鍵の生成、符号化処理、暗号化処理のいずれをも電子配信事業者２が行う場合である。

【０３２７】

いずれの運用形態の場合も、鍵情報の配信主体に誰がなるかにかかわらず、結局のところ暗号鍵を知り得る立場にある者は配給権者１と電子配信事業者２の２者となる。なおこの場合も既存の配信モデルに比してシステムの安全性を確保できる。

【０３２８】

【発明の効果】

（１）請求項１～５のいずれかに記載の発明によれば、各配信者に固有の複数の鍵情報を発生し、これら複数の鍵情報をディジタルデータとは別の配信経路であって、かつ鍵情報相互においても別の配信経路となるように、すなわち複数の配信経路を用いて個別に配信することにより、暗号鍵を復元するのに必要な全ての情報を一度に入手するのが困難な配信方法を実現できる。また下流側システムを、暗号処理の解除されたディジタルデータにスクランブル処理を施して出力する復号サーバと、当該スクランブル処理を解除する出力装置とで構成することにより、復号サーバと出力装置を結ぶ伝送路上でも不正複製が困難な配信方法を実現できる。

【０３２９】

（２）請求項６に記載の発明によれば、下流側システムを、暗号処理の解除されたディジタルデータにスクランブル処理を施して出力する復号サーバと、当該スクランブル処理を解除する出力装置とで構成することにより、復号サーバと出力装置を結ぶ伝送路上でも不正複製が困難な下流側システムを実現できる。

【０３３０】

（３）請求項７に記載の発明によれば、その出力信号からはディジタルデータの不正複製が困難な復号サーバを実現できる。また、請求項８に記載の発明によれば、当該回路装置を電子機器に搭載するだけで請求項７の復号サーバと同様の機能を実現できる。また、請求項９に記載の発明によれば、専用装置を用いなくても、請求項７の復号サーバと同様の機能を実現することができる。また、請求

項１０に記載の発明によれば、スクランブル制御部と別途組み合わせることで、請求項７の復号サーバと同様の機能を容易に実現可能な復号サーバを実現できる。同様に、請求項１１に記載の発明によれば、当該回路装置とスクランブル制御部とを別途組み合わせて電子機器に搭載するだけで請求項７の復号サーバと同様の機能を実現できる。また、請求項１２に記載の発明によれば、コンピュータをスクランブル制御部として機能させるプログラムと組み合わせることで、専用装置を用いなくても、請求項７の復号サーバと同様の機能を実現することができる。また、請求項１３に記載の発明によれば、請求項１０に記載の発明と組み合わせることで、請求項７の復号サーバと同様の機能を容易に実現可能な復号サーバを実現できる。同様に、請求項１４に記載の発明によれば当該回路装置と請求項１１に記載の回路装置とを別途組み合わせて電子機器に搭載するだけで請求項７の復号サーバと同様の機能を実現できる。また、請求項１５に記載の発明によれば、請求項１２に記載のプログラムと組み合わせることで、専用装置を用いなくても、請求項７の復号サーバと同様の機能を実現することができる。

【０３３１】

（４）請求項１６に記載の発明によれば、その入力信号からはディジタルデータの不正複製が困難な出力装置を実現できる。また、請求項１７に記載の発明によれば、当該回路装置を電子機器に搭載するだけで請求項１６の出力装置と同様の機能を実現できる。また、請求項１８に記載の発明によれば、専用装置を用いなくても、請求項１６の出力装置と同様の機能を実現することができる。

【０３３２】

（５）請求項１９に記載の発明によれば、復号サーバが暗号処理の解除されたディジタルデータにスクランブル処理を施して出力する仕組みを採用し、他方、出力装置がディジタルデータに施されているスクランブル処理を解除して所定の出力形態で出力する仕組みを採用することにより、復号サーバと出力装置の伝送路上でも不正複製が困難な下流側システムにおける信号処理方法を実現できる。

【０３３３】

（６）請求項２０に記載の発明によれば、復号サーバが暗号処理の解除されたディジタルデータにスクランブル処理を施して出力する仕組みを採用することに

より、その出力信号からはディジタルデータの不正複製が困難な復号サーバにおける信号処理方法を実現できる。

【図面の簡単な説明】

【図１】

本発明にかかる配信システムの概念を説明する概念構成図である。

【図２】

本発明にかかる配信システムにおける高速配信用ネットワークで配信されるデータのデータ構造を示す図である。

【図３】

本発明にかかる配信システムを映画コンテンツに適用した場合について示す図である。

【図４】

本発明の実施の形態における第１の配信システムの構成例を示すブロック図である。

【図５】

本発明の実施の形態における第２の配信システムの構成例を示すブロック図である。

【図６】

本発明の実施の形態における第３の配信システムの構成例を示すブロック図である。

【図７】

本発明の実施の形態における第４の配信システムの構成例を示すブロック図である。

【図８】

本発明の実施の形態における第５の配信システムの構成例を示すブロック図である。

【図９】

本発明の実施の形態における第６の配信システムの構成例を示すブロック図である。

【図１０】

本発明の実施の形態における第７の配信システムの構成例を示すブロック図である。

【図１１】

本発明の実施の形態における第８の配信システムの構成例を示すブロック図である。

【図１２】

本発明の実施の形態における第９の配信システムの構成例を示すブロック図である。

【図１３】

本発明の実施の形態における第１０の配信システムの構成例を示すブロック図である。

【図１４】

本発明の実施の形態における第１１の配信システムの構成例を示すブロック図である。

【図１５】

本発明の実施の形態における第１２の配信システムの構成例を示すブロック図である。

【図１６】

本発明の実施の形態における第１３の配信システムの構成例を示すブロック図である。

【図１７】

本発明の実施の形態における第１４の配信システムの構成例を示すブロック図である。

【図１８】

本発明の実施の形態の構成例として示す各配信システムに共通する運用形態を表示した図である。

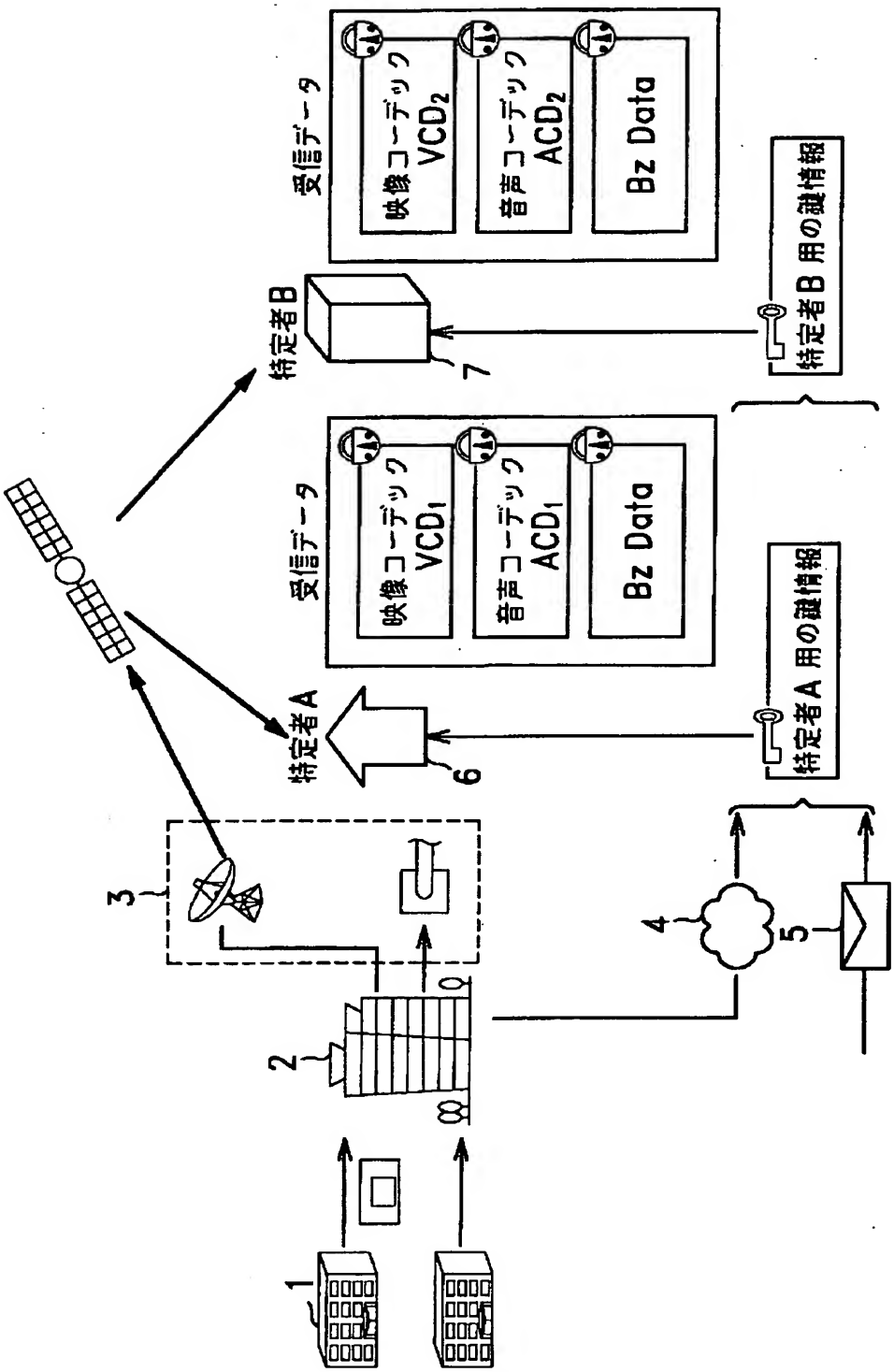
【符号の説明】

１　コンテンツサーバ、１２　コンテンツ符号化部、１３　暗号化部、１４

送出サーバ、１５　コンテンツ管理サーバ、１６　鍵発生部、１７　配信先管理サーバ、１８，２６　合わせ鍵生成部、１９，２１，２２，２５，２７，２８，２９　書込部、２０　部分鍵生成部、２３　多重鍵生成部、２４　鍵暗号化処理部、３１　受信サーバ、３２，３８，３９，４０，４１，４２，４３　読取部、３３　復号サーバ、３４　出力装置、３４Ａ　デスクランブル部、３５　復号機能部、３５Ａ　復号化部、３５Ｂ　鍵復元部、３５Ｃ　コンテンツ復号化部、３５Ｄ　スクランブル部、３６　スクランブル制御部、３７　出力ログ管理部

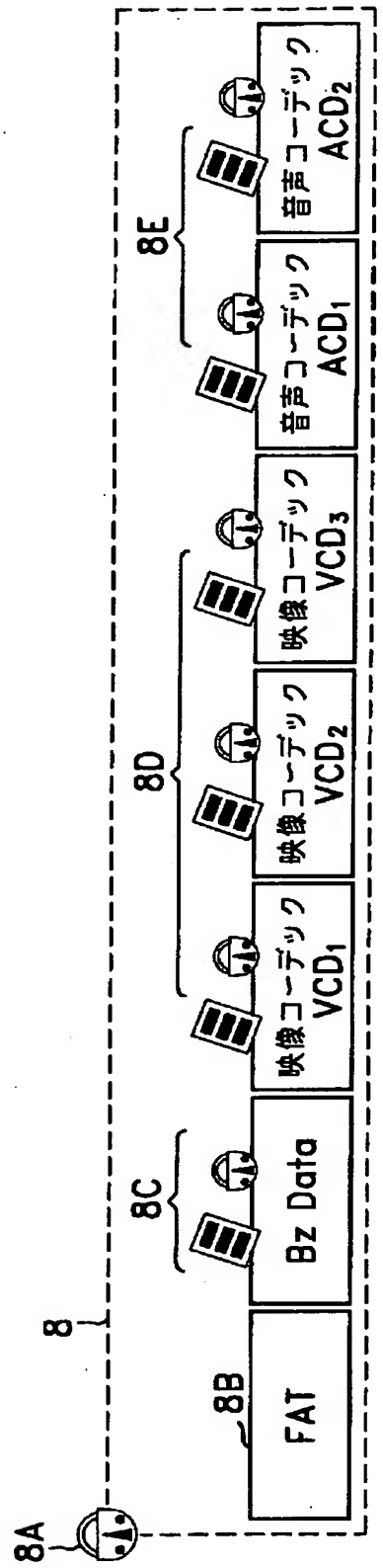
【書類名】　　図面

【図１】



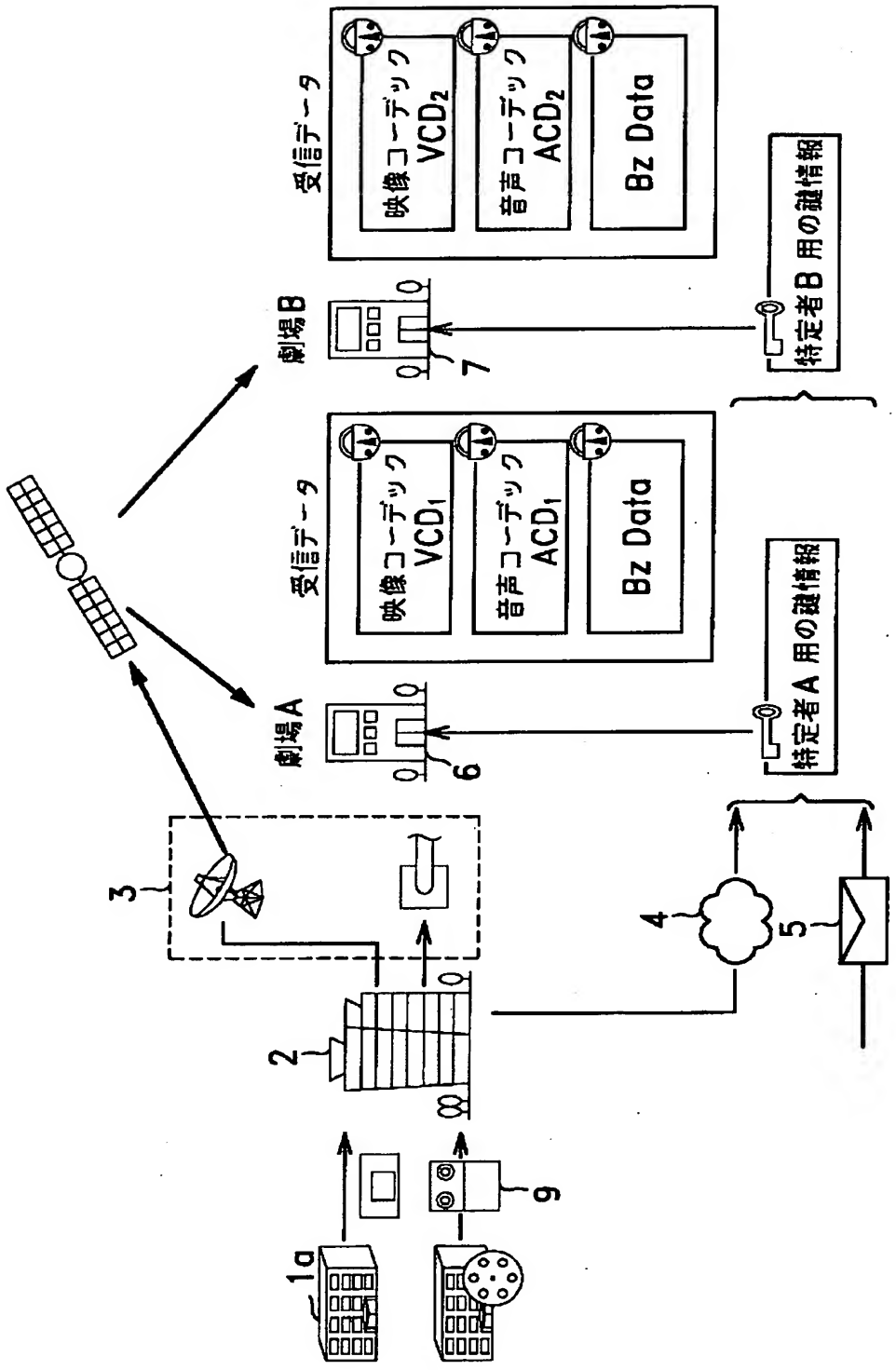
出証特２００１－３０２７４５９

【図２】

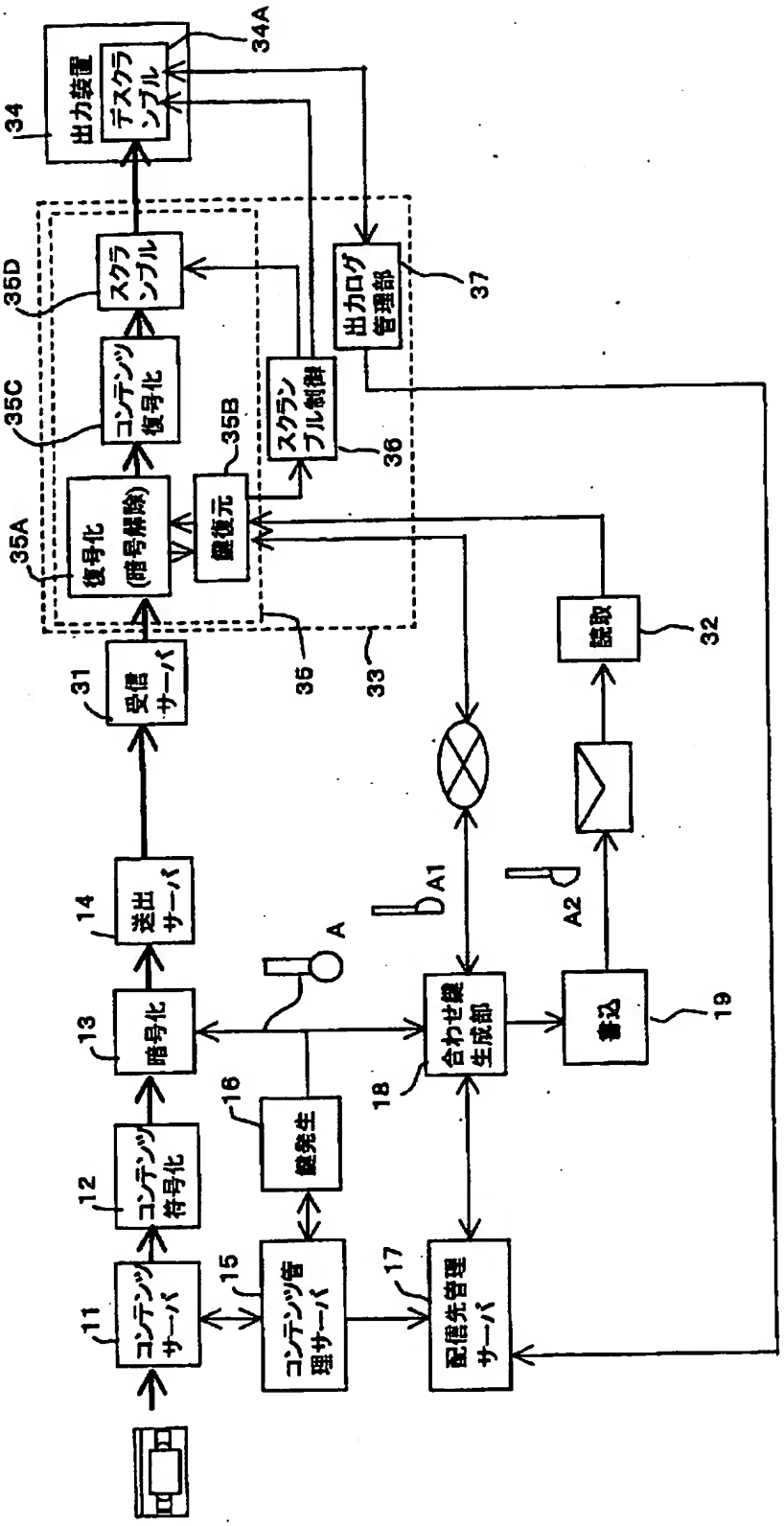


出証特２００１－３０２７４５９

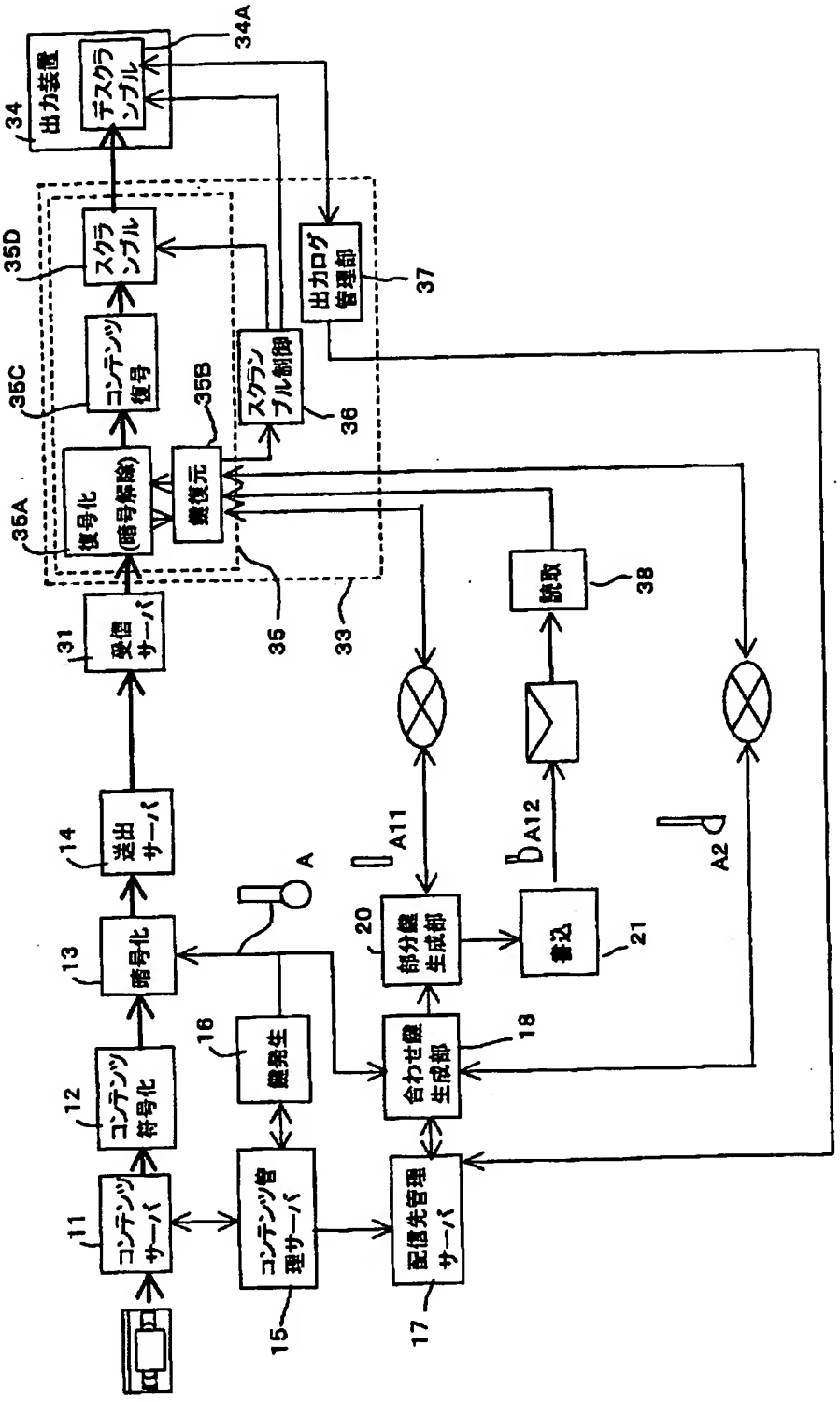
【図３】


受信データ
映像コーデック VCD2
音声コーデック ACD2
Bz Data
劇場B
7
特定者B用の鍵情報
受信データ
映像コーデック VCD1
音声コーデック ACD1
Bz Data
劇場A
6
特定者A用の鍵情報
3
4
5
2
9
1a

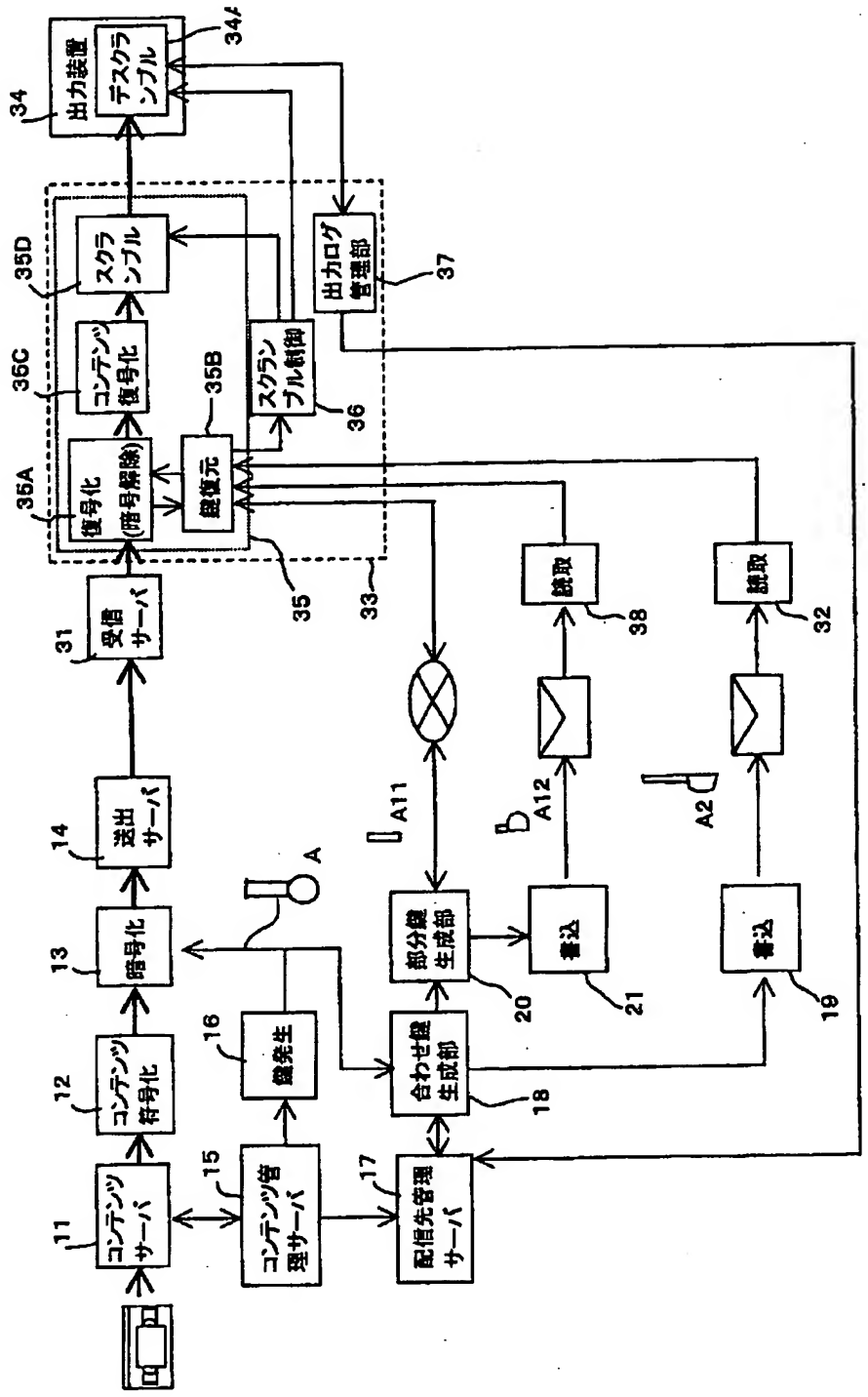
【図４】


出力装置
34
デスクランブル
34A
スクランブル
35D
コンテンツ復号化
35C
復号化(暗号解除)
35A
鍵復元
35B
スクランブル制御
36
出力ログ管理部
37
受信サーバ
31
送出サーバ
14
暗号化
13
コンテンツ符号化
12
コンテンツサーバ
11
コンテンツ管理サーバ
15
鍵発生
16
配信先管理サーバ
17
合わせ鍵生成部
18
書込
19
読取
32
A
A1
A2
33
36

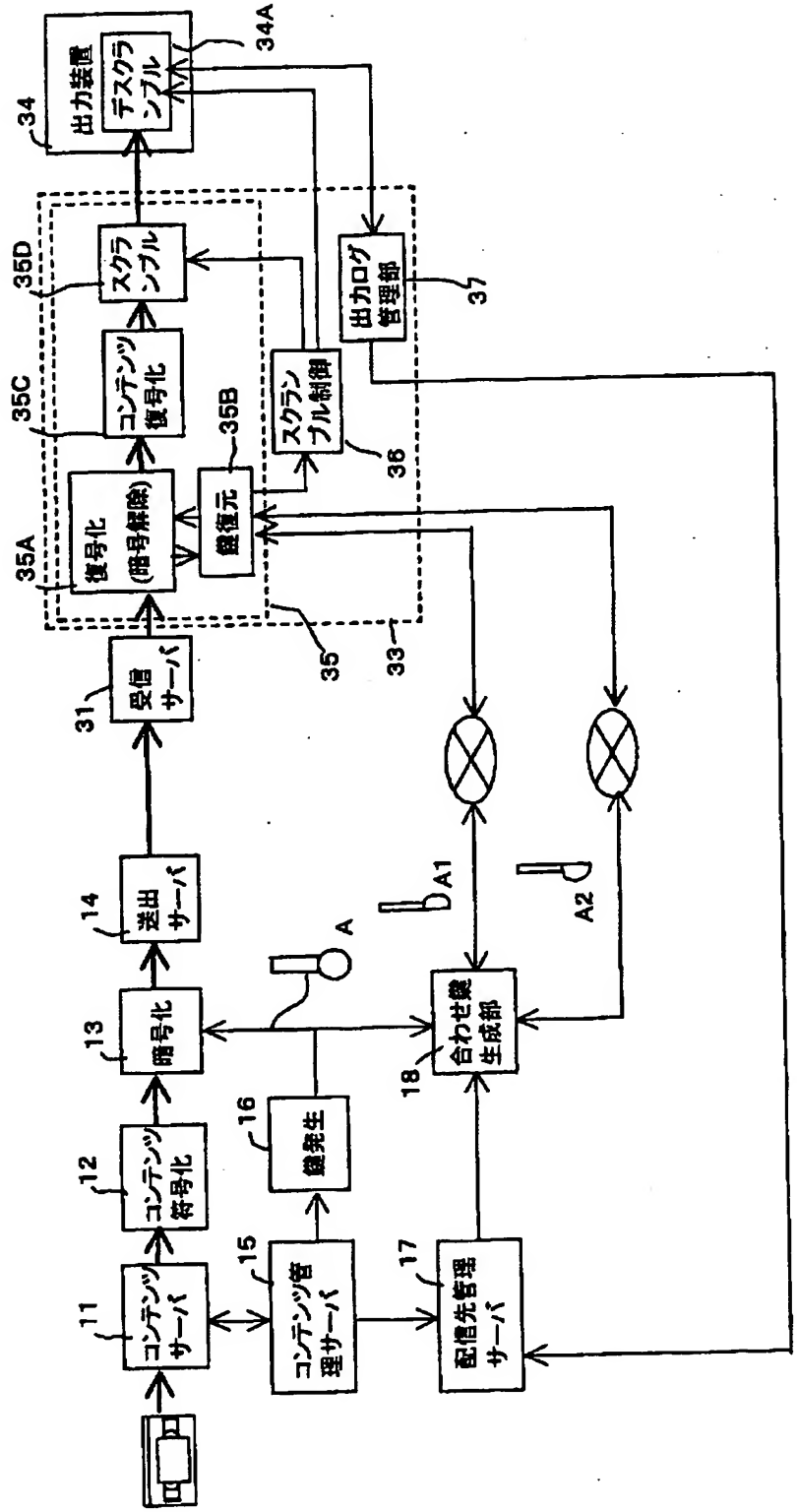
【図５】


34
出力装置
デスクランブル
34A
35D
スクランブル
35C
コンテンツ復号
35B
スクランブル制御
36
出力ログ管理部
37
35A
復号化（暗号解除）
鍵復元
35
33
31
受信サーバ
14
送出サーバ
13
暗号化
A
A11
A12
A2
20
部分鍵生成部
21
書込
読取
38
12
コンテンツ符号化
16
鍵発生
18
合わせ鍵生成部
11
コンテンツサーバ
コンテンツ管理サーバ
15
配信先管理サーバ
17

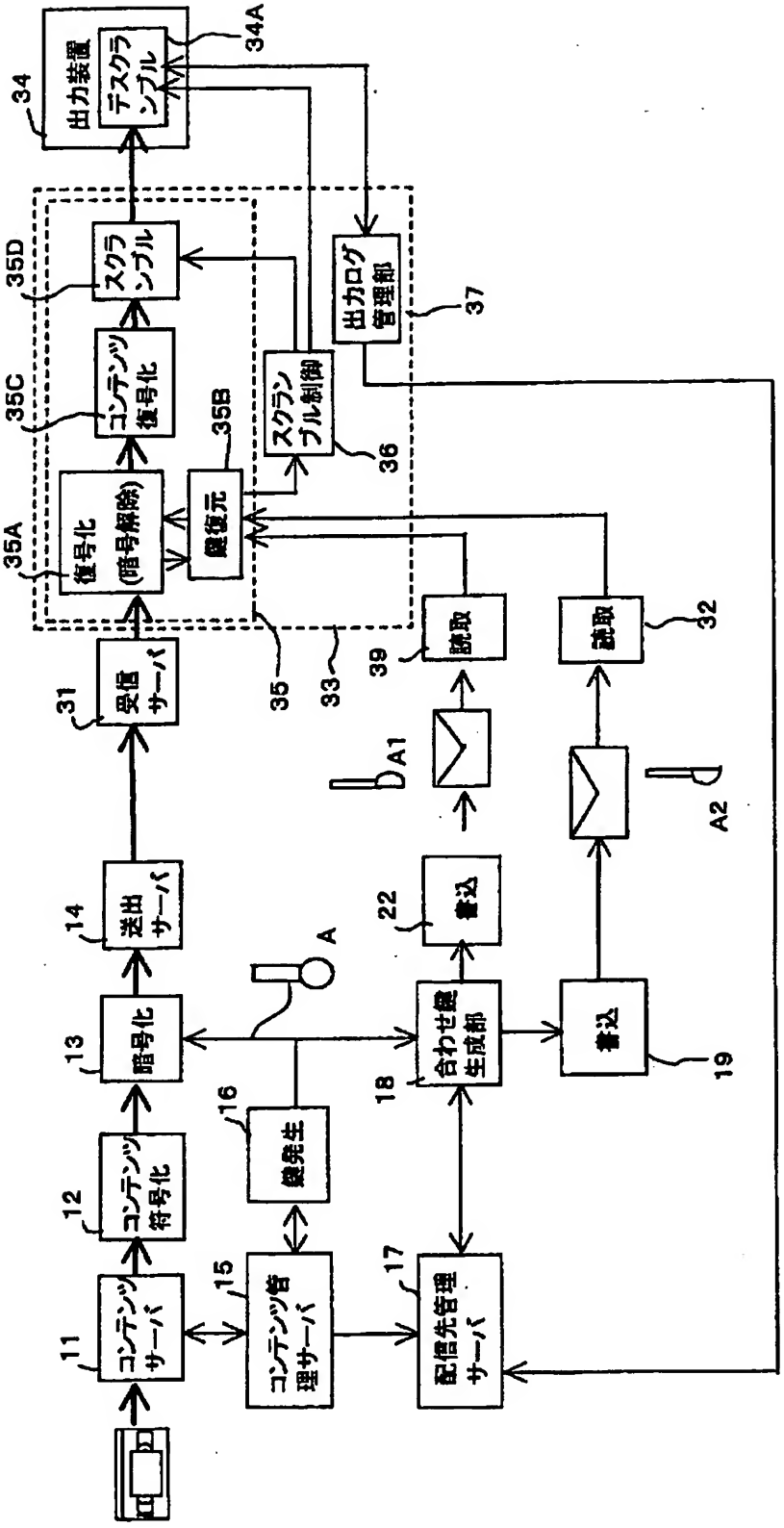
【図６】


出力装置
デスクラシブル
34
34A
スクラシブル
35D
コンテンツ復号化
35C
復号化(暗号解除)
35A
鍵復元
35B
スクランブル制御
36
出力ログ管理部
37
35
33
受信サーバ
31
送出サーバ
14
暗号化
13
コンテンツ符号化
12
コンテンツサーバ
11
コンテンツ管理サーバ
15
鍵発生
16
配信先管理サーバ
17
合わせ鍵生成部
18
部分鍵生成部
20
書込
21
書込
19
A
A11
A12
A2
B
読取
38
読取
32

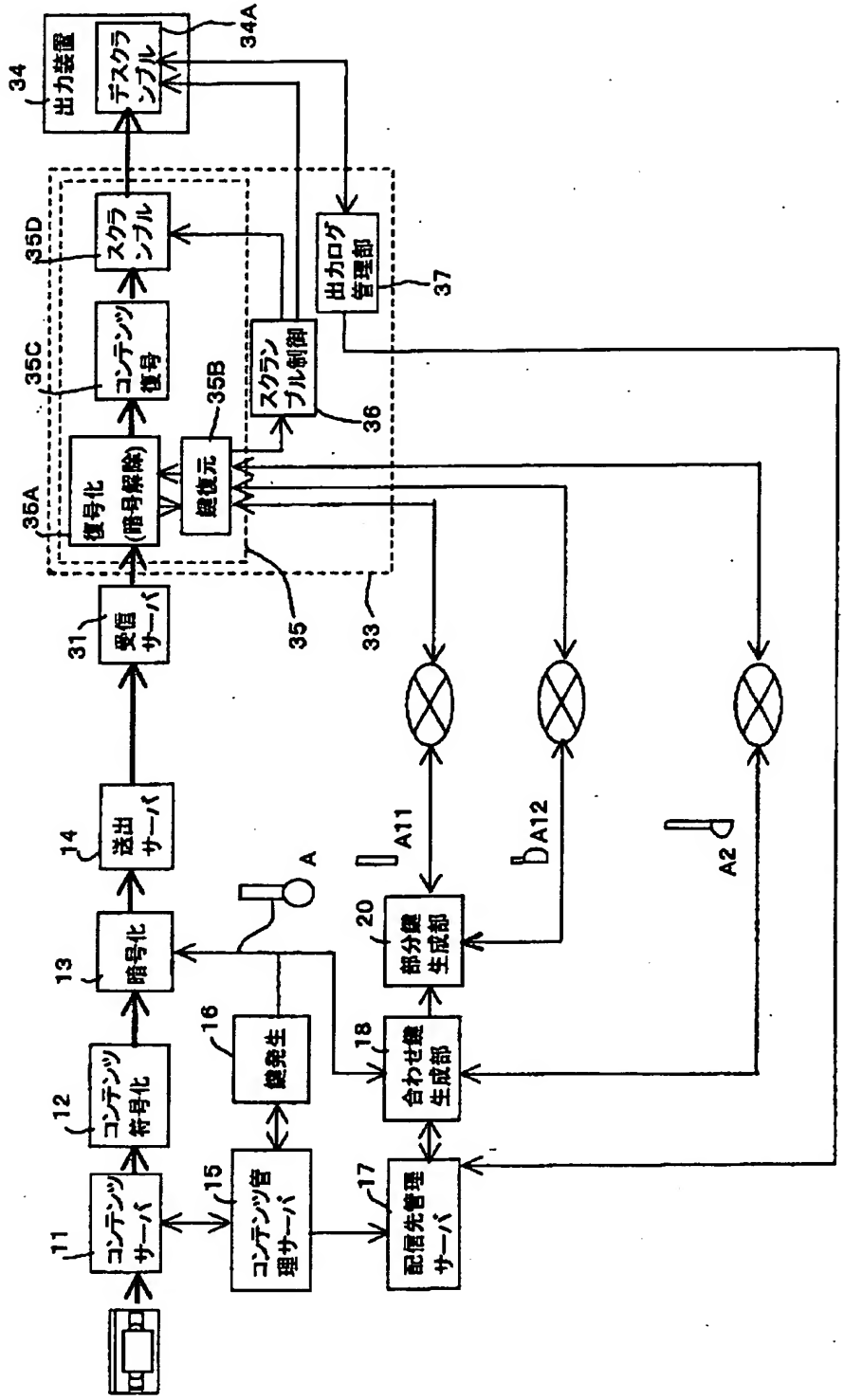
【図７】


出力装置
デスクラシブル
34
34A
スクラシブル
35D
コンテンツ復号化
35C
復号化(暗号解除)
35A
鍵復元
35B
スクランブル制御
36
出力ログ管理部
37
35
33
受信サーバ
31
送出サーバ
14
暗号化
13
コンテンツ符号化
12
コンテンツサーバ
11
A
鍵発生
16
コンテンツ管理サーバ
15
合わせ鍵生成部
18
配信先管理サーバ
17
bA1
dA2

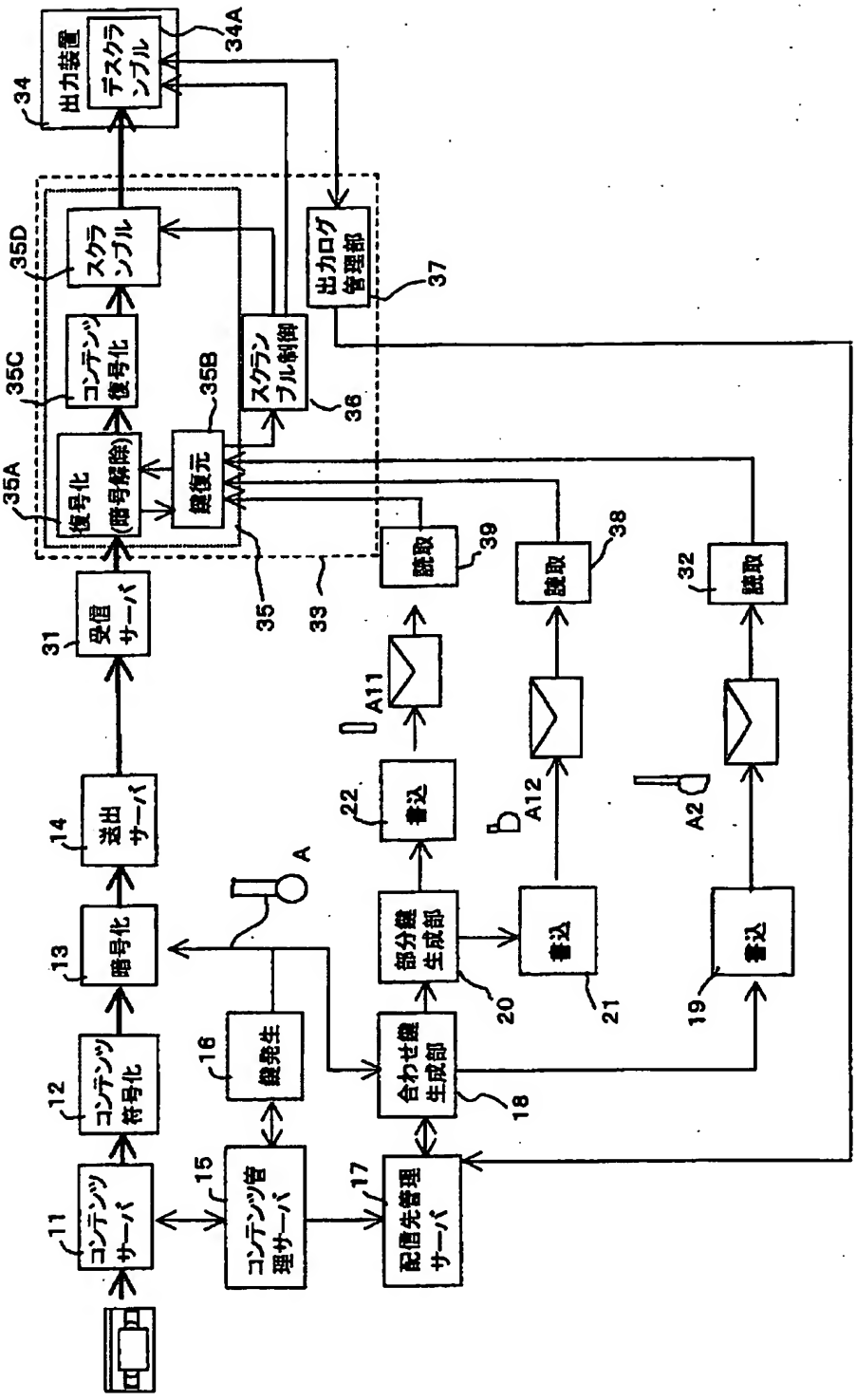
【図８】


出力装置
デスクランブル
34A
34
スクランブル
35D
コンテンツ復号化
35C
復号化(暗号解除)
35A
鍵復元
35B
スクランブル制御
36
出力ログ管理部
37
受信サーバ
31
35
33
39
読取
読取
32
A1
A2
送出サーバ
14
22
書込
A
暗号化
13
合わせ鍵生成部
18
書込
19
鍵発生
16
コンテンツ符号化
12
コンテンツ管理サーバ
15
配信先管理サーバ
17
コンテンツサーバ
11

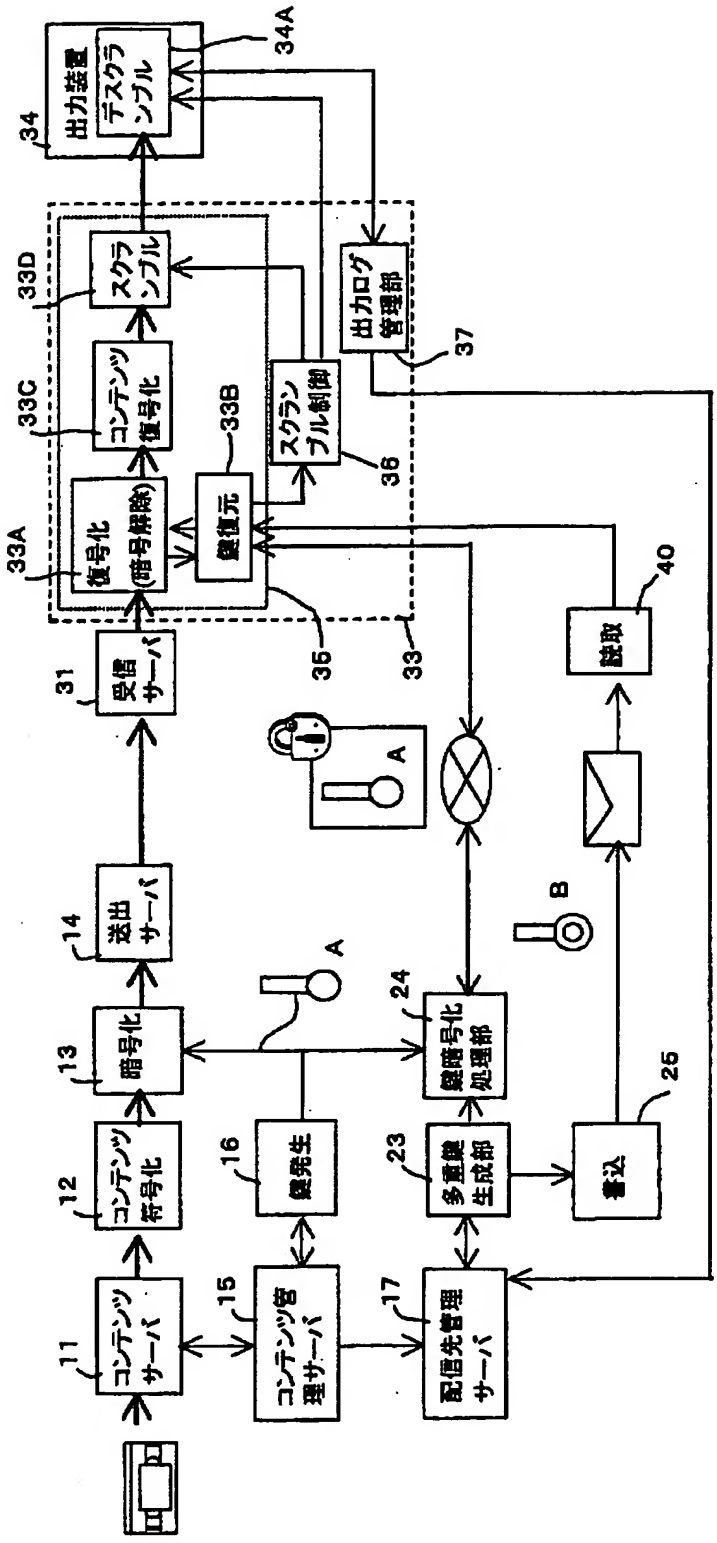
【図９】


34
出力装置
34A
デスクランブル
35D
スクランブル
35C
コンテンツ復号
35B
鍵復元
35A
復号化(暗号解除)
35
33
36
スクランブル制御
出力ログ管理部
37
31
受信サーバ
14
送出サーバ
13
暗号化
12
コンテンツ符号化
11
コンテンツサーバ
15
コンテンツ管理サーバ
16
鍵発生
17
配信先管理サーバ
18
合わせ鍵生成部
20
部分鍵生成部
A
A11
A12
A2

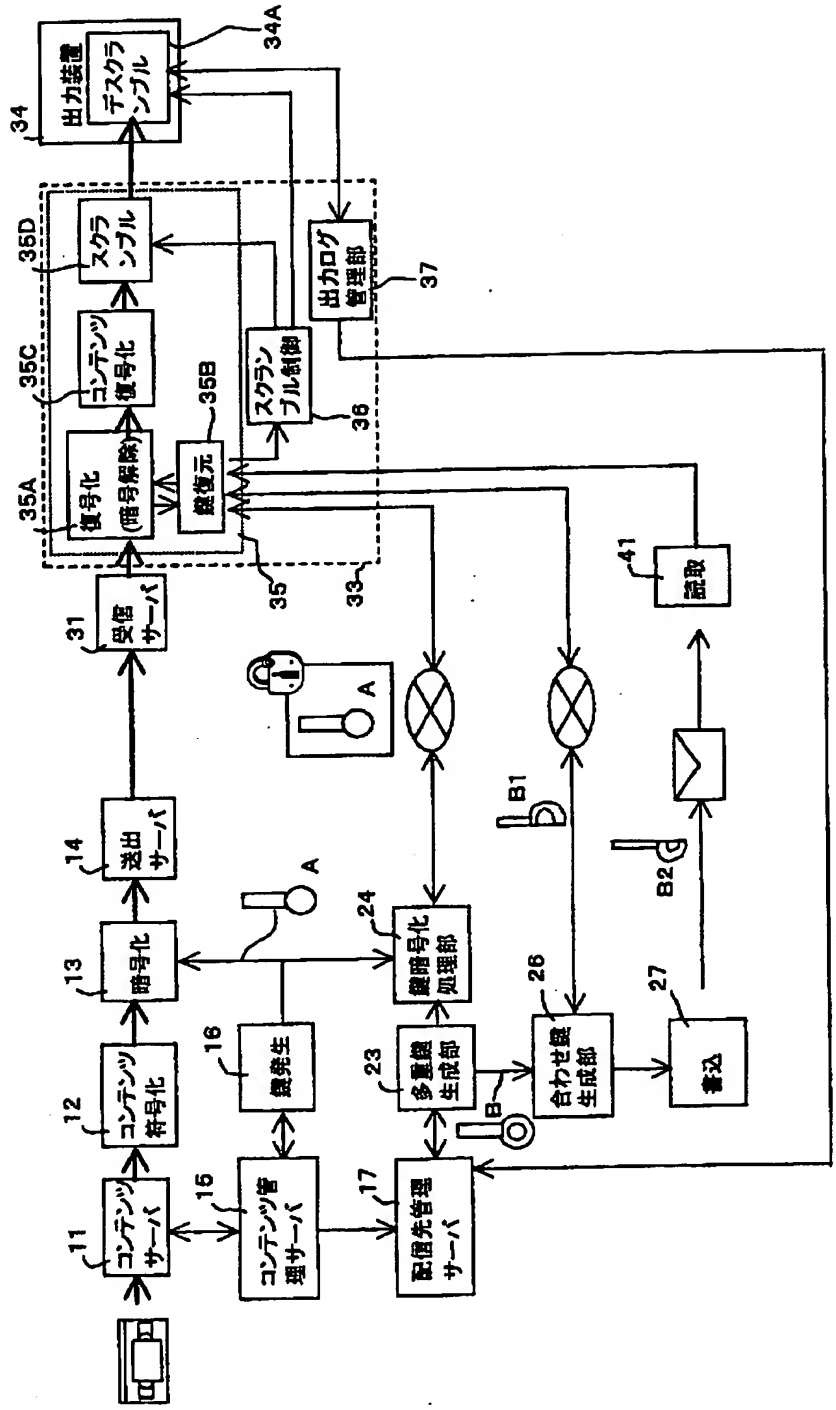
【図１０】


出力装置
デスクランブル
34A
34
出力ログ管理部
37
スクランブル制御
36
スクランブル
35D
コンテンツ復号化
35C
復号化(暗号解除)
35A
鍵復元
35B
受信サーバ
31
35
33
読取
39
読取
38
読取
32
A11
A12
A2
送出サーバ
14
書込
22
書込
21
書込
19
暗号化
13
部分鍵生成部
20
A
コンテンツ符号化
12
鍵発生
16
合わせ鍵生成部
18
コンテンツサーバ
11
コンテンツ管理サーバ
15
配信先管理サーバ
17

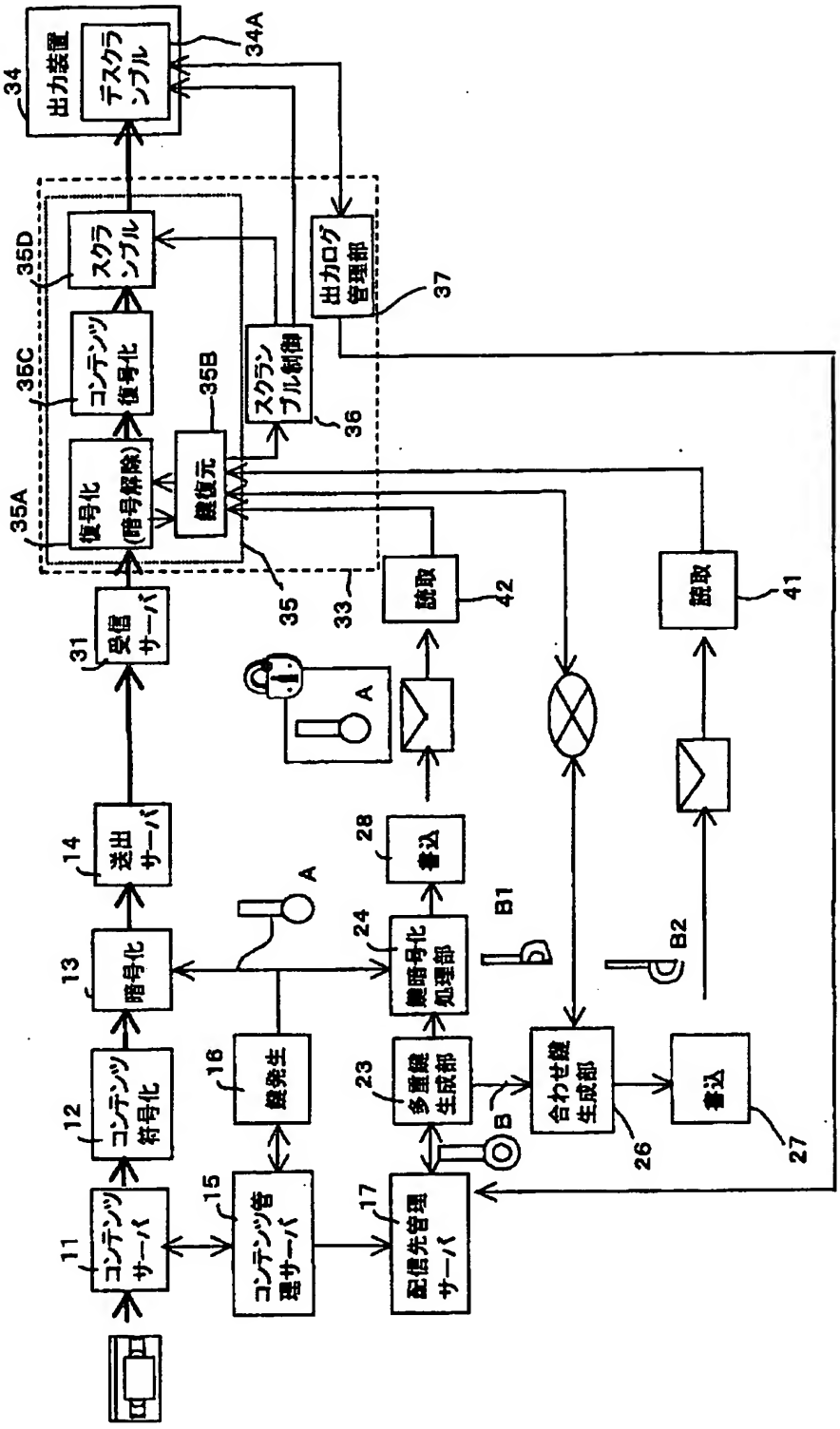
【図１１】


出力装置
デスクラシブル
34
34A
スクラシブル
33D
コンテンツ復号化
33C
復号化(暗号解除)
33A
鍵復元
33B
スクランブル制御
出力ログ管理部
36
37
33
受信サーバ
31
送出サーバ
14
暗号化
13
コンテンツ符号化
12
コンテンツサーバ
11
鍵発生
16
コンテンツ管理サーバ
15
鍵暗号化処理部
24
多重鍵生成部
23
配信先管理サーバ
17
書込
25
旋取
40
A
B

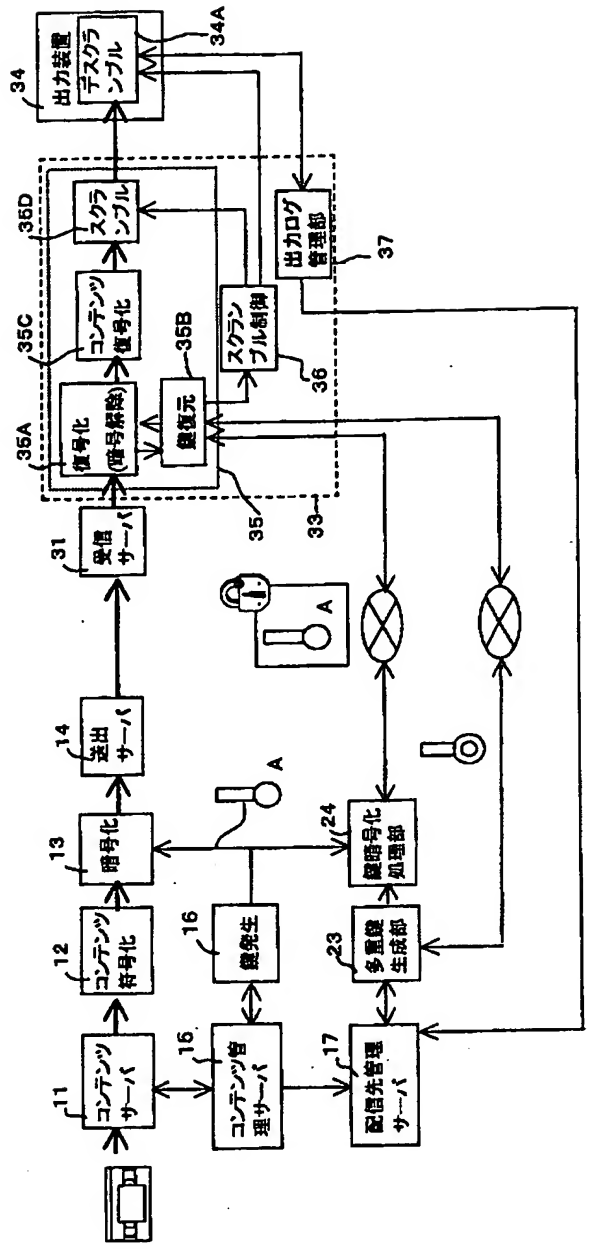
【図１２】


出力装置
デスクランブル
34
34A
スクランブル
35D
コンテンツ復号化
35C
復号化（暗号解除）
35A
鍵復元
35B
スクランブル制御
36
出力ログ管理部
37
受信サーバ
31
35
33
課金
41
送出サーバ
14
暗号化
13
コンテンツ符号化
12
コンテンツサーバ
11
鍵発生
16
コンテンツ管理サーバ
15
鍵暗号化処理部
24
多重鍵生成部
23
配信先管理サーバ
17
合わせ鍵生成部
26
書込
27
A
B1
B2
B

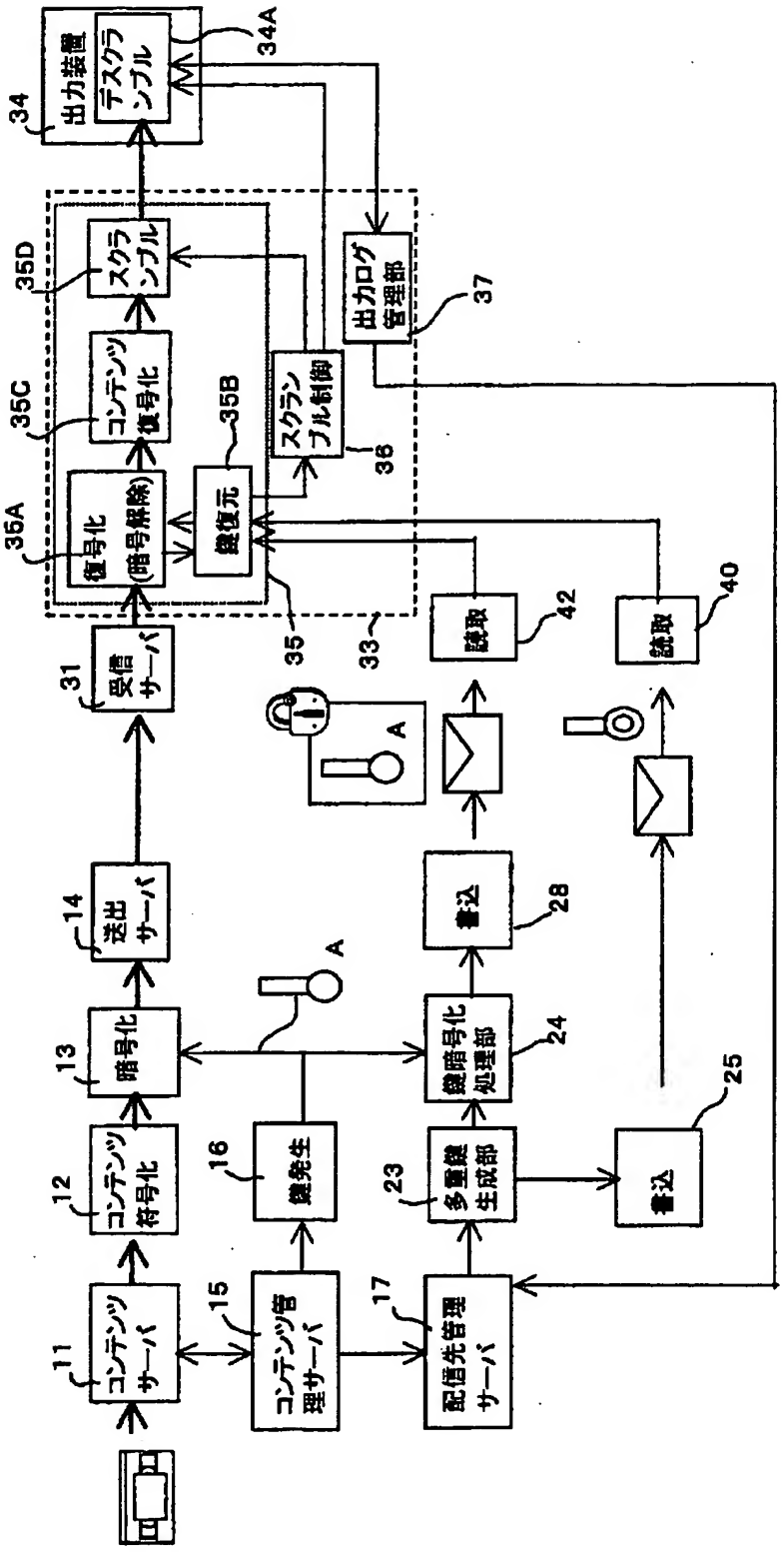
【図１３】


34
出力装置
デスクラシンプル
34A
35D
スクラシンプル
35C
コンテンツ復号化
35B
スクランブル制御
出力ログ管理部
37
36
35A
復号化（暗号解除）
鍵復元
35
33
読取
42
読取
41
31
受信サーバ
A
28
書込
14
送出サーバ
A
B1
B2
24
鍵暗号化処理部
13
暗号化
18
鍵発生
23
多重鍵生成部
合わせ鍵生成部
26
書込
27
12
コンテンツ符号化
B
15
コンテンツ管理サーバ
17
配信先管理サーバ
11
コンテンツサーバ

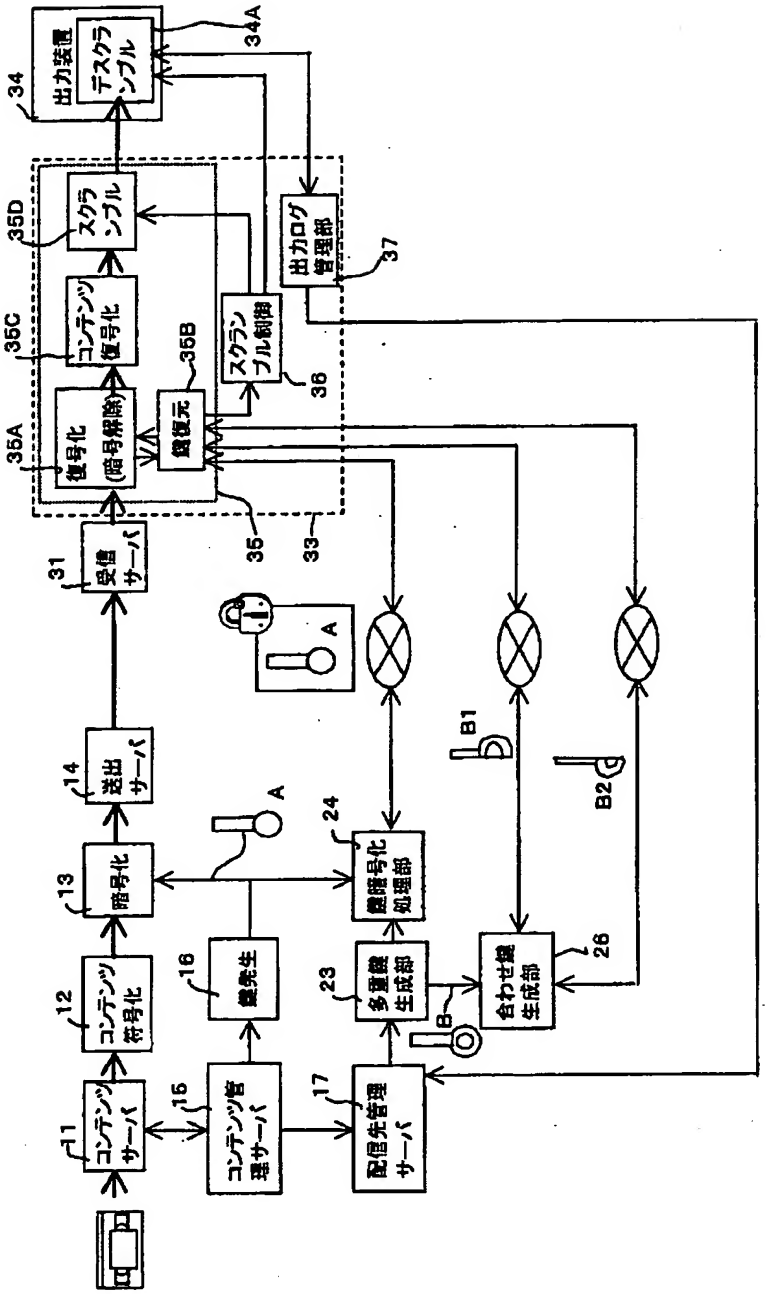
【図１４】


34
出力装置
デスクランブル
34A
35D
スクランブル
35C
コンテンツ復号化
35B
鍵復元
35A
復号化（暗号解除）
スクランブル制御
出力ログ管理部
37
36
35
33
31
受信サーバ
A
14
送出サーバ
A
13
暗号化
24
鍵暗号化処理部
12
コンテンツ符号化
16
鍵発生
23
多重鍵生成部
11
コンテンツサーバ
16
コンテンツ管理サーバ
17
配信先管理サーバ

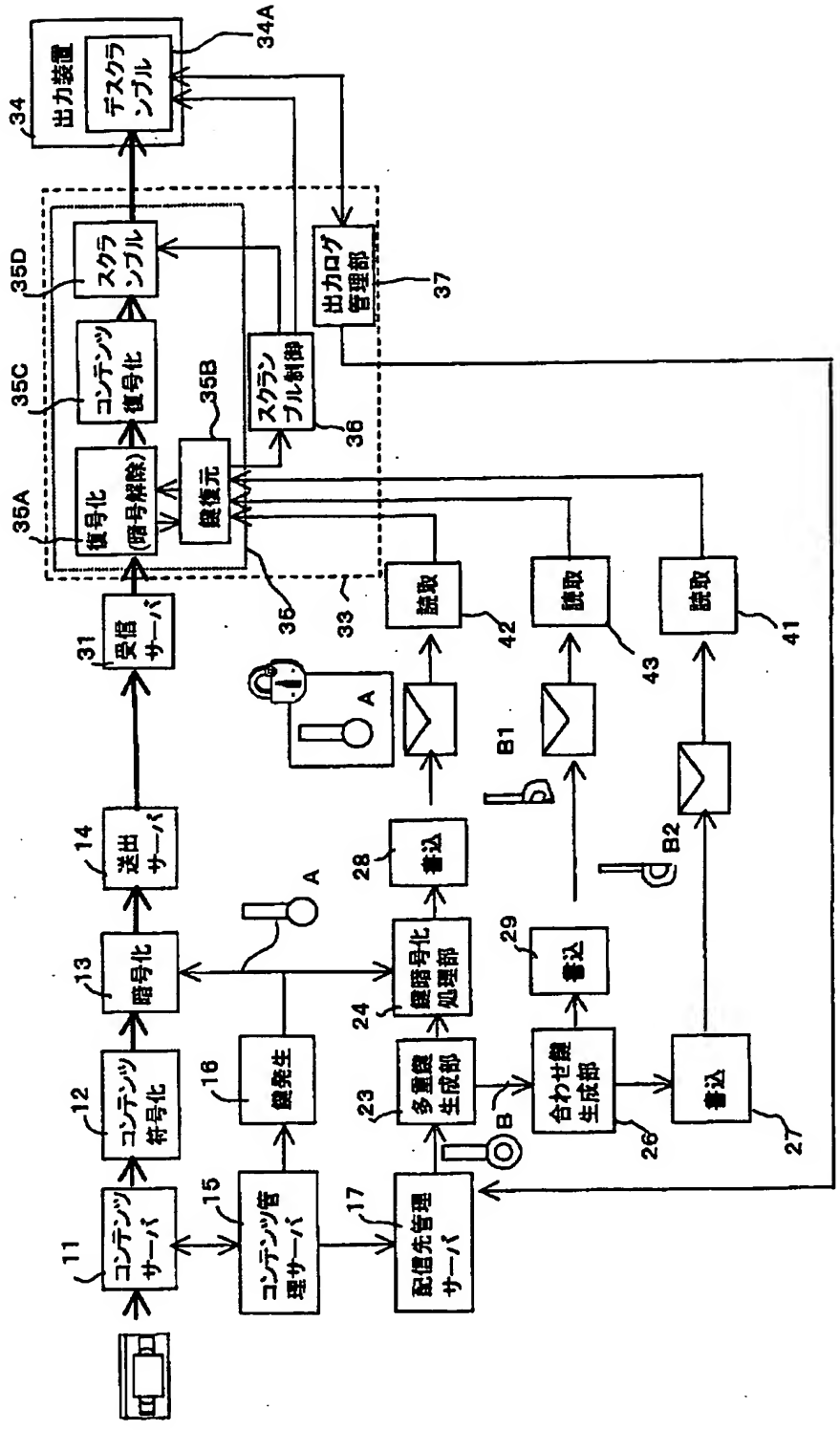
【図１５】


34
出力装置
デスクランブル
34A
35D
スクランブル
出力ログ管理部
37
35C
コンテンツ復号化
35B
スクランブル制御
38
35A
復号化(暗号解除)
鍵復元
35
33
31
受信サーバ
読取
42
読取
40
A
14
送出サーバ
書込
28
A
13
暗号化
鍵暗号化処理部
24
12
コンテンツ符号化
16
鍵発生
23
多重鍵生成部
書込
25
11
コンテンツサーバ
15
コンテンツ管理サーバ
17
配信先管理サーバ

【図１６】


34
出力装置
デスクランブル
34A
35D
スクランブル
35C
コンテンツ復号化
35B
復元
35A
復号化
(暗号解除)
スクランブル制御
36
出力ログ管理部
37
35
33
31
受信サーバ
A
B1
B2
14
送出サーバ
A
24
13
暗号化
暗号化処理部
16
鍵発生
23
多重鍵生成部
B
合わせ鍵生成部
26
12
コンテンツ符号化
11
コンテンツサーバ
15
コンテンツ管理サーバ
17
配信先管理サーバ

【図１７】


出力装置
34
デスクラ
ンブル
34A
出力ログ
管理部
37
スクラ
ンブル
35D
コンテンツ
復号化
35C
スクラン
ブル制御
35B
36
復号化
(暗号解除)
35A
鍵復元
受信
サーバ
31
送出
サーバ
14
暗号化
13
コンテンツ
符号化
12
コンテンツ
サーバ
11
コンテンツ管
理サーバ
15
鍵発生
16
配信先管理
サーバ
17
多重鍵
生成部
23
鍵暗号化
処理部
24
合わせ鍵
生成部
26
書込
28
書込
29
書込
27
読取
42
読取
43
読取
41
A
B
B1
B2
33

【図１８】

	暗号鍵の発生者	符号化実行者	暗号化実行者	鍵情報の配信者	配給権者から見たシステムの安全性	備考
1	制作者	制作者	制作者	制作者(2つ)	+++	
2	同上	同上	同上	制作者(1つ)+配信者(1つ)	++	配信者が暗号化された暗号鍵を入手
3	同上	同上	同上	配信者(2つ)	++	配信者が暗号鍵を入手して鍵情報を作成
4	同上	同上	配信者	制作者(2つ)	++	暗号鍵は配信者に通知される
5	同上	同上	同上	制作者(1つ)+配信者(1つ)	++	同上
6	同上	同上	同上	配信者(2つ)	++	同上
7	同上	配信者	同上	制作者(2つ)	++	同上
8	同上	同上	同上	制作者(1つ)+配信者(1つ)	++	同上
9	同上	同上	同上	配信者(2つ)	++	同上
10	配信者	制作者	制作者	制作者(2つ)	+	制作者が暗号鍵を入手して鍵情報を作成
11	同上	同上	同上	制作者(1つ)+配信者(1つ)	+	同上
12	同上	同上	同上	配信者(2つ)	+	同上
13	同上	同上	配信者	制作者(2つ)	+	同上
14	同上	同上	同上	制作者(1つ)+配信者(1つ)	+	同上
15	同上	同上	同上	配信者(2つ)	+	同上
16	同上	配信者	同上	制作者(2つ)	+	同上
17	同上	同上	同上	制作者(1つ)+配信者(1つ)	+	同上
18	同上	同上	同上	配信者(2つ)	+	同上

【書類名】　要約書

【要約】

【課題】　不正行為の困難性とランニングコストの低減要求を両立する。

【解決手段】　復号サーバにおいて暗号処理の解除が許可されるとき、復号サーバ内で発生されたスクランブル鍵を用いて、暗号処理の解除されたディジタルデータをスクランブル処理する。このようにスクランブル処理の施されたディジタルデータを出力装置に与えることで、復号サーバと出力装置とを分離しても、当該伝送経路上で不正行為を行えないようにする。

【選択図】　図４

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社